VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Nasazení IP telefonních Honeypotů v reálné infrastruktuře

Deploying IP telephony honeypots in real infrastructure

2016 **Bc. Zuzana Bajáková**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Zuzana Bajáková**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Nasazení IP telefonních Honeypotů v reálné infrastruktuře
Deploying IP Telephony Honeypots in Real Infrastructure

Jazyk vypracování: čeština

Zásady pro vypracování:

Bezpečnost IP telefonie je v současné době aktuálním problémem. Komunikační servery jsou často cílem útoků za účelem získat přístup k uživatelským účtům a touto cestou poté realizovat finanční újmu vlastníkovi. Cílem diplomové práce je analyzovat data z Honeypotů, které budou zapojeny v síti s vysokou intenzitou provozu a budou sloužit jako monitorovací prostředí pro příchozí útoky. Ty mohou být generovány uměle pomocí série penetračních testů, nebo se bude jednat o útoky z reálného prostředí. Následnou důkladnou statistikou budou definovány nejčastěji používané typy hrozeb a budou vytvořeny praktická protiopatření, která by útoky v praxi omezila, či úplně eliminovala.

1. Nastudujte detailně problematiku VoIP, bezpečnost signalizace SIP a RTP protokolu.
2. Proveďte detailní rešerši nástrojů pro implementaci VoIP Honeypot.
3. Popište a realizujte zapojení Honeypot v praktické infrastruktuře.
4. Proveďte statistiku útoků z reálného prostředí.
5. Vypracujte teoretický návrh bezpečnostních protiopatření na základě výsledků statistiky.

Seznam doporučené odborné literatury:

[1] M. Collier, D. Endler - Hacking Exposed Unified Communications & VoIP Security Secrets & Solutions, Second Edition, 2013

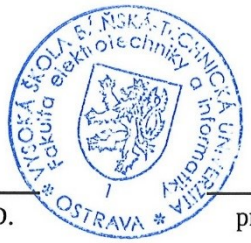
[2] N. Provos, T. Holz - Virtual Honeypots: From Botnet Tracking to Intrusion Detection, 2007

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Filip Řezáč**

Datum zadání: 01.09.2015

Datum odevzdání: 29.04.2016



doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

V Ostravě dne: *21. dubna 2016*

.....
podpis studenta

Poďakovanie

Touto cestou by som chcela vyjadriť vďaku všetkým, ktorí mi v akejkoľvek miere pomohli pri tvorbe tejto práce, predovšetkým však Ing. Filipovi Řezáčovi za jeho cenné rady, ochotnú pomoc pri riešení problémov, poskytnutie materiálov a odborné vedenie, a tiež Ing. Jakubovi Šafaříkovi za poskytnutie dát pre analýzu útokov.

Abstrakt

Diplomová práca je zameraná na bezpečnosť v internetovej telefónii a analýzu útokov. Hlavným cieľom bolo analyzovať dáta zachytené v reálnej prevádzke. Na začiatku sú objasnené základné pojmy VoIP technológie a problematika bezpečnostných rizík. Ďalej práca definuje pojem honeypot, jeho využitie a delenie do rôznych kategórií. Sú tiež uvedené nástroje pre realizáciu honeypotov v IP telefónii. Obsahom tejto práce je aj štatistická analýza útokov na SIP protokol v rôznych geograficky i logicky oddelených sieťach. Záver práce je venovaný výsledkom analýzy a návrhu vhodných bezpečnostných protiopatrení.

Kľúčové slová

bezpečnostné riziká, Dionaea, DoS, honeypot, IP telefónia, neurónová sieť, paketový analyzér, RTP, real-time prenos, SIP bezpečnosť, SIP signalizácia, sonda, štatistická analýza, Tcpdump, UDP, útoky, VoIP

Abstract

Diploma thesis is focused on security in internet telephony and analysis of attacks. The main objective of this thesis was to analyze data captured in real traffic. At the beginning, basic components of VoIP technology and security risks are clarified. Thesis defines honeypot concept, its use and division into different categories. It also describes tools for implementing honeypots in IP telephony. This work includes statistical analysis of attacks on SIP protocol in various geographically and logically separate networks. The final part contains results of analysis and theoretical design of appropriately secured network.

Key words

attacks, Dionaea, DoS, honeypot, IP telephony, neural network, packet analyzer, probe, RTP, real-time transfer, safety risks, SIP safety, SIP signalization, statistical analysis, Tcpdump, UDP, VoIP

Obsah

Zoznam použitých skratiek

Skratka	Význam
3DES	Triple Data Encryption Standard. Metóda šifrovania dát.
AES	Advanced Encryption Standard. Metóda šifrovania dát.
DHCP	Dynamic Host Configuration Protocol. Súbor zásad, ktorý umožňuje zariadeniam vyžiadanie a získanie IP adresy od servera.
DNS	Domain Name System. Systém ukladajúci prístup k informáciám o názve stroja a domény.
DoS	Denial of Service. Druh útoku na zariadenie alebo službu v sieti.
HTTP	Hypertext Transfer Protocol. Protokol pre prenos dokumentov medzi klientmi a servermi služby World Wide Web.
HTTPS	Hypertext Transfer Protocol Secure. Zabezpečený HTTP protokol.
ICMP	Internet Control Message Protocol. Protokol pre odosielanie chybových správ.
ID	Identifikačné číslo.
IDS	Instruction Detection System. Systém pre odhalenie prieniku.
IP	Internet Protocol. Základný komunikačný protokol internetu.
IPS	Instruction Prevention System. Systém pre detekciu a prevenciu útoku.
IPsec	IP security. Bezpečnostné rozšírenie IP protokolu.
IPv4	Internet Protocol version 4. Štvrtá verzia internetového protokolu.
IPv6	Internet Protocol version 6. Štiesta verzia internetového protokolu.
MD5	Message-Digest algorithm 5. Hashovacia funkcia.
MLP	MultiLayer Perceptron. Viacvrstvá neurónová sieť.
MSSQL	Microsoft Structured Query Language Server. Databázový a analytický systém.
OS	Operačný systém.
OSI	Open Systems Interconnection Reference Model. Model rozdeľujúci sieťové protokoly do vrstiev.
PBX	Private Branch eXchange. Pobočková telefónna ústredňa.
RFC	Request For Comments. Dokumenty s odporúčaniami pre fungovanie internetu.
RSA	Rivest, Shamir, Adleman. Šifra s verejným kľúčom.
RTP	Real-time Transport Protocol. Protokol pre komunikáciu v reálnom čase.
S/MIME	Secure/Multipurpose Internet Mail Extensions. Bezpečnostné rozšírenie štandardu pre odosielanie e-mailových správ.
SHA-1	Secure Hash Algorithm 1. Hashovacia funkcia.
SIP	Session Initiation Protocol. Signalizačný protokol pre multimediálne spojenie cez internet.
SIPS	SIP over TLS. Bezpečnostný mechanizmus prevzatý z HTTPS protokolu.
SMB	Server Message Block. Sieťový komunikačný protokol.
SMTP	Simple Mail Transfer Protocol. Protokol zaisťujúci prenos e-mailov.
SPIT	Spam over Internet Telephony. Spam v internetovej telefónii.

SRTP	Secure RTP. Zabezpečený protokol prenosu v reálnom čase.
SSH	Secure Shell. Sieťový protokol pre zabezpečenú dátovú komunikáciu.
SW	Software.
TFTP	Trivial File Transfer Protocol. Jednoduchý protokol pre prenos súborov medzi počítačmi obsahujúci základné funkcie protokolu FTP.
TLS	Transport Layer Security. Protokol slúžiaci na šifrovanie dát.
UA	User Agent. Koncové zariadenie v SIP infraštruktúre.
UAC	User Agent Client. Koncové zariadenie v SIP infraštruktúre na strane klienta.
UAS	User Agent Server. Koncové zariadenie v SIP infraštruktúre na strane servera.
UDP	User Datagram Protocol. Protokol pre prenos datagramov v sieti.
URI	Uniform Resource Identifier. Reťazec znakov používaný pre identifikáciu zdroja.
VLAN	Virtual Local Area Network. Virtuálna lokálna sieť.
VoIP	Voice over Internet Protocol. Technológia pre prenos hlasu prostredníctvom internetového protokolu.
VPN	Virtual Private Network. Virtuálna privátna sieť, prepojenie dôveryhodných sietí cez nedôveryhovnú.
WAV	Waveform audio file format. Zvukový formát.
ZRTP	Zimmermann RTP. Nadstavbový protokol pre SRTP.

Zoznam ilustrácií a zoznam tabuliek

Úvod

S rastúcou popularitou komunikácie pomocou IP telefónie narastá aj počet útočníkov a tiež nové metódy narúšania siete. Bezpečnosť býva v týchto prípadoch často podceňovaná a tak je nezabezpečený prenos hlasu cez Internet ľahko odpočúvateľný. Okrem koncových zariadení bývajú často napádané komunikačné servery, kedy sa útočníci snažia získať prístup k užívateľským účtom a tie následne zneužívajú. Pre dostatočnú ochranu VoIP technológie je nutné držať krok s hackermi a neprestávať zlepšovať bezpečnostné opatrenia. Z tohoto dôvodu bol vyvinutý nástroj honeypot, ktorého hlavnou vlastnosťou je odhaľovanie nedostatočného zabezpečenia a získavanie informácií o priebehu útoku.

Táto diplomová práca nadväzuje na moju bakalársku prácu, ktorej cieľom bol prieskum vhodných honeypotov použiteľných pre IP telefóniu. Tieto honeypoty boli otestované pomocou umelo generovaných penetračných testov, pričom na základe ich funkčnosti bolo výsledkom bakalárskej práce odporúčanie tých najvhodnejších nástrojov pre nasadenie do reálnej siete. Táto diplomová práca je v úvode venovaná základným pojmom IP telefónie, čitateľ je oboznámený s technológiou Voice over IP a s protokolmi, ktoré táto služba využíva. Sú nimi hlavne signalizačný protokol SIP (Session Initiation Protocol), transportný RTP protokol (Real-time Transport Protocol) a ich bezpečnostné mechanizmy. Tieto pojmy je nutné poznať pre hlbšie pochopenie ďalšieho textu. Druhá kapitola sa zaoberá problematikou bezpečnostných rizík vo VoIP SIP telefónii, ktorými sú monitoring a manipulácia so signalizáciou, či útoky ako Man in the Middle a DoS (Denial od Service). V ďalšej časti je definovaný pojem honeypot, jeho využitie a delenie do rôznych kategórií. Sú popísané nástroje pre implementáciu VoIP honeypotov Artemisa a Dionaea a tiež paketový analyzér Tcpdump. Vo štvrtej kapitole je čitateľ zoznámený s podkladmi meraní a tiež so základným popisom neurónovej siete. Následne je táto kapitola venovaná spôsobom, ktorými budú dáta získané z honeypotov a spracované neurónovou sieťou analyzované. Jedná sa o porovnávanie počtu zachytených útokov rôznymi sondami, ich pôvodu, zisťovanie najvyužívanejšieho typu útoku na VoIP technológiu a popis exploračnej analýzy a štatistickej indukcie. V záverečnej časti sú uvedené jednotlivé výsledky analýzy dát a tiež teoretický návrh vhodných bezpečnostných protiopatrení.

Hlavným cieľom tejto diplomovej práce je analýza dát z VoIP honeypotov nasadených v reálnej sieti s vysokou intenzitou prevádzky, keďže najlepšou možnosťou, ako získať relevantné informácie o chovaní útočníkov je analýza reálnych dát. Cieľom práce je takisto definícia najčastejšie používaných typov útokov a teoretický návrh protiopatrení, ktoré by v praxi mohli dané útoky obmedziť či úplne eliminovať.

1 IP telefónia

Táto kapitola rieši problematiku Voice over IP a protokolov, ktoré táto služba využíva, konkrétne bezpečnosť signalizácie SIP a transportného RTP protokolu. Riešiť túto problematiku je potrebné pre hlbšie porozumenie bezpečnosti v internetovej telefónii, ktorej budú venované nadchádzajúce kapitoly. Vzhľadom na to, že VoIP je v podstate mladou technológiou, je jej zabezpečenie stále vyvíjané. Protokoly, ktoré VoIP využíva, vo svojej základnej podobe neobsahujú zabezpečovacie mechanizmy, a sú tým pádom nechránené. Preto je potrebné navrhovať zabezpečovacie techniky pre signalizačné a transportné protokoly.

Voice over Internet Protocol - VoIP je technológia umožňujúca prenos signalizácie a hlasu, ktorý je digitalizovaný, cez internetový protokol. Využíva sa pre telefonovanie prostredníctvom internetu alebo iných paketovo prepínaných sietí, pričom sú dáta rozdelené do jednotlivých IP paketov. Pre samotný prenos sa využíva IP protokol tretej vrstvy modelu OSI. Každý paket je vybavený záhlavím, ktoré obsahuje cieľovú adresu a je samostatne prenášaný sieťou. Rôzne pakety môžu byť prenášané po rôznych cestách, nemusia do cieľa doraziť v rovnakom poradí v akom boli vyslané zo zdroja a niektoré sa môžu stratiť. Pri takomto prenose sa používa kompresia hlasu, čím sa zmenšuje potrebná prenosová rýchlosť. Je tiež možné prekladanie hlasových a dátových paketov. V cieli sú následne jednotlivé pakety poskladané do podoby pôvodného hlasového signálu. Táto technológia pre signalizáciu a vyjednanie parametrov spojenia používa protokoly SIP a SDP. Pre real-time prenos dát štandardne používa protokoly UDP (User Datagram Protocol), RTP.

UDP je jednoduchý protokol transportnej vrstvy OSI modelu. V IP telefónii sa používa pre rýchly a nenáročný prenos dát, podporuje dvojstrannú komunikáciu, ako aj komunikáciu jedného účastníka s viacerými. Nezaručuje však, že dáta dorazia do cieľa v rovnakom poradí, v akom boli odoslané, nezaisťuje potvrdzovanie o doručení a tým pádom ani samotné doručenie dát. Spoľahlivosť prenosu preto musí byť zaistená ďalšími protokolmi, vo VoIP sa tak využíva protokol RTP.

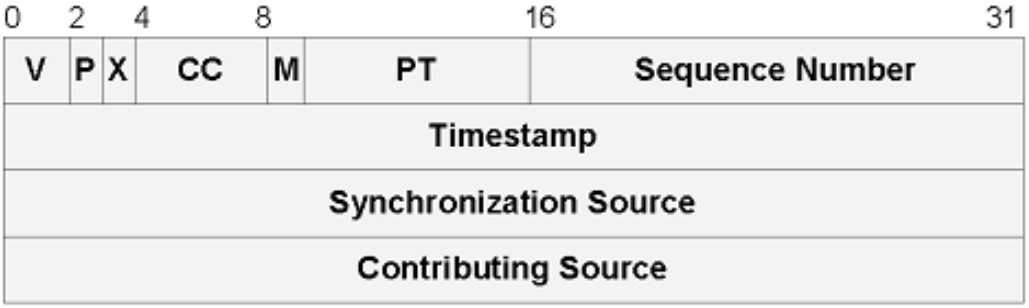
Na obrázku 1.1 je zobrazená štruktúra správy používaná pre prenos v reálnom čase.

Obr. 1.1 Štruktúra správy pre prenos v reálnom čase.

1.1 RTP

RTP je v RFC 1889 definovaný ako nespojovo orientovaný transportný protokol. Využíva transportný protokol UDP, ktorého prenos vylepšuje. Slúži pre prenos audio/video dát v reálnom čase, zaisťuje zoradenie zasielaných paketov (Sequence Number) a ich časové značkovanie (Timestamp), ďalej tiež multiplexovanie a demultiplexovanie. Samotný audio/video prenos je dopĺňaný o kontrolný protokol RTCP (Real Time Control Protocol), ktorý nesie informácie o priebehu prenosu – zhromažďuje štatistiky prenosu, informácie o množstve odoslaných bajtov a počte paketov, stratených paketov a tiež o rozptyle meškania. Protokol RTP dokáže prenášať dáta v unicastovej aj multicastovej prevádzke. Ako je možné vidieť na obrázku 1.2, RTP paket sa skladá z nasledujúcich položiek:

- V – verzia protokolu
- P – doplnenie o jeden či viac doplnkových oktetov na koci paketu, ktoré nenesú žiadne užitočné dáta
- X – rozširujúci bit
- CC (CSRC Count) – číslo identifikátoru príspevku zdroja
- M - značka
- PT (Payload Type) – typ paketu. Definuje formát a určenie prenášaných dát.
- Sequence Number – číslo odosielaného paketu. Každým odoslaným RTP paketom sa jeho hodnota zvyšuje o jeden. Slúži pre správne zostavenie doručenej správy a pre určenie prípadnej straty paketu.
- Timestamp – čas odobratia prvého vzorku prenášaného RTP paketom. Časový údaj sa neodoberá zo systémového času, ale zo zdroja dát z dôvodu synchronizácie a korekcie rozptylu meškania.
- Synchronization Source – synchronizačné číslo zdroja dát. Jedná sa o jedinečné, náhodne vygenerované číslo.
- Contributing Source – zoznam identifikujúci prispievacie zdroje

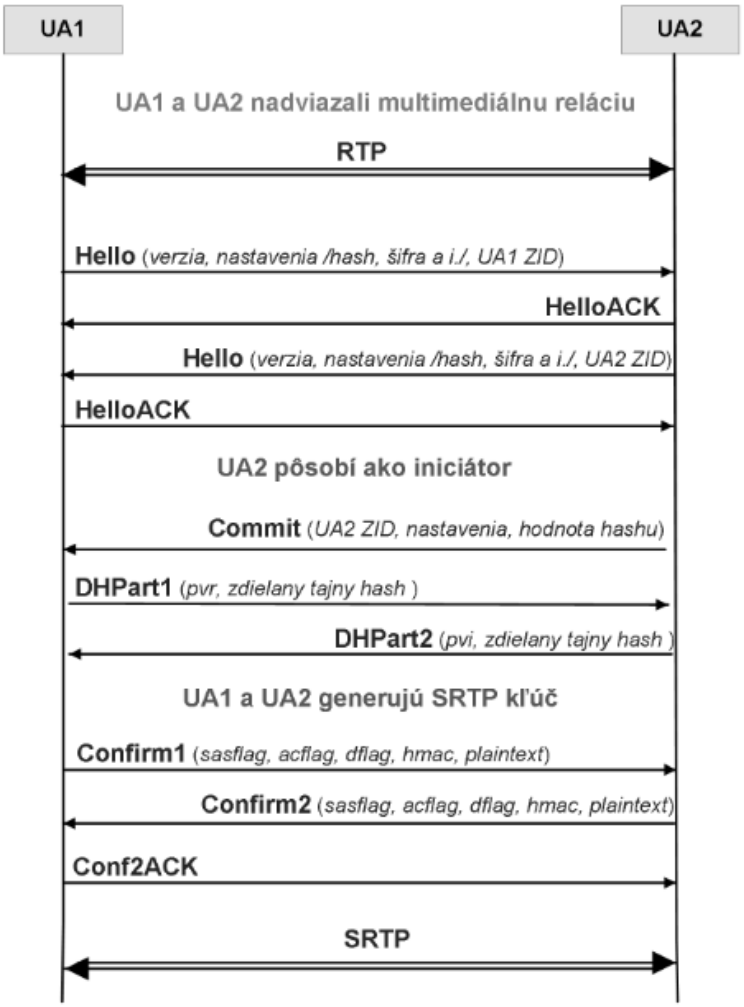


Obr. 1.2 RTP paket.

1.1.1 SRTP, ZRTP

Nešifrovaným prenosom pomocou RTP sa zvyšuje riziko odpočúvania hovoru. A keďže samotný RTP protokol neobsahuje žiadne ochranné mechanizmy, bol vyvinutý protokol SRTP (Secure Real-time Transport Protocol). Ten obsahuje bezpečnostné mechanizmy ako podpora integrity, overenie autenticity, zaručenie dôvernosti či ochrana proti preposlaniu. Prenášaný obsah je zašifrovaný symetrickou šifrou AES, integrita polí hlavičiek je zaistená pomocou autentizačnej značky získanej algoritmom HMAC-SHA-1 (Hashed Message Authentication Code – SHA-1).

ZRTP (Zimmermann Real-time Transport Protocol) je nadstavbou SRTP protokolu pre jeho ľahšie použitie a implementáciu. Pri výmene kľúčov používa Diffie-Hellmanov algoritmus. Ten slúži na vytvorenie a bezpečnú výmenu zdieľaného tajného kľúča, ktorý bude následne využitý pre symetrické šifrovanie prenášaných dát. ZRTP pracuje v troch fázach, v ktorých detekuje podporu ZRTP implementácie ostatnými účastníkmi, nasleduje výmena hodnôt pre dohodu na kľúčoch pomocou Diffie-Hellmanovho algoritmu a nakoniec sa komunikácia prepne do SRTP módu, ako je vidieť na obrázku 1.3.



Obr. 1.3 Využitie ZRTP pre zostavenie SRTP spojenia.

1.2 SIP

SIP je signalizačný protokol, ktorý sa využíva pre zostavenie, modifikáciu a ukončenie spojenia s jedným alebo s viacerými účastníkmi. Pracuje na aplikačnej vrstve, je jednoducho implementovateľný, rozšíriteľný a flexibilný. Tento protokol je end-to-end orientovaný, koncové zariadenia poznajú jednotlivé stavy komunikácie, čím sa zvyšuje odolnosť voči chybám. Je typu klient-server, pričom pod pojmom klient si môžeme predstaviť IP telefón či SW aplikáciu a pojmom server je označený aplikačný server služieb. Samotná komunikácia medzi klientom a serverom prebieha výmenou dvoch typov správ: žiadostí (klient → server) a odpovedí (server → klient). Tie sú obvykle prenášané v datagramoch UDP protokolu. Transakcia je zobrazená na obr. 1.4.

V jadre SIP protokolu je podľa RFC 3261 špecifikovaných šesť žiadostí (okrem nich existuje aj niekoľko ďalších, ktoré sú definované inými RFC):

INVITE je žiadosť o nadviazanie spojenia alebo zmenu parametrov už prebiehajúceho spojenia. Telo správy obsahuje jeho popis.

ACK potvrdzuje prijatie konečnej odpovede na žiadosť INVITE.

BYE je správa, ktorou klient oznamuje, že chce ukončiť nadviazané spojenie.

CANCEL je metóda využívaná pre zrušenie spojenia v prípade, keď volaný ešte nepotvrdil konečnou odpoveďou žiadosť INVITE a nie je zostavený dialóg.

REGISTER je žiadosť o registráciu užívateľa. Registrácie sú časovo limitované, je preto nutné ich periodicky obnovovať.

OPTIONS je metóda pre zistenie vlastností SIP zariadenia. Má rovnakú štruktúru ako metóda INVITE, no nie je zostavované spojenie.

Na každú žiadosť musí byť odpoveď, výnimkou je len metóda ACK. Kód odpovede je celé číslo z rozsahu 100 až 699 a značí jej typ. Definovaných je celkom 6 tried:

1xx sú dočasné informatívne odpovede
(100 Trying, 180 Ringing, ...)

2xx sú pozitívne finálne odpovede
(200 OK, 202 accepted: Used for referals)

3xx sú odpovede využívané na presmerovanie
(300 Multiple Choices, 301 Moved Permanently, ...)

4xx sú negatívne konečné odpovede znamenajúce problém na strane klienta
(400 Bad Request, 404 Not Found: User not found, ...)

5xx sú negatívne konečné odpovede a znamenajú problém na strane servera
(500 Server Internal Error, 502 Bad Gateway,...)

6xx predstavujú globálnu chybu
(600 Busy Everywhere, 606 Not Acceptable, ...)

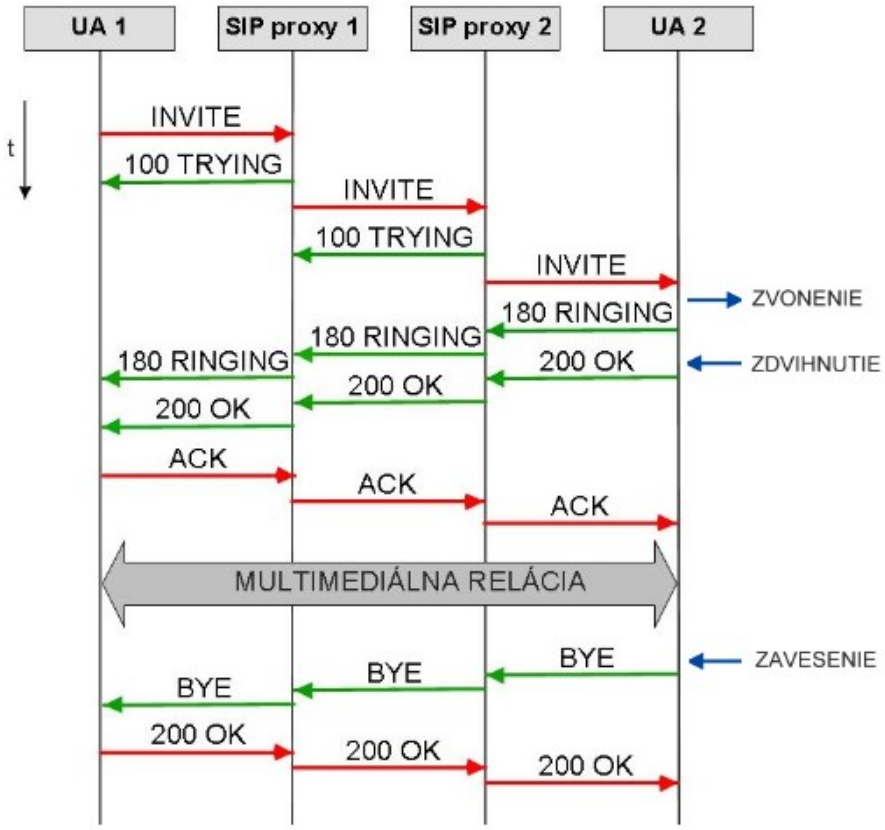
Základnými prvkami SIP siete sú:

- SIP user agent (UA) - koncové body, na ktorých vzniká SIP relácia. Obvykle sú predstavované koncovými terminálmi vo forme SW SIP telefónu či aplikáciami. Každý UA obsahuje UAC (User Agent Server) a UAS (User Agent Client)
- SIP proxy, registrar, redirect a location servery, v praxi implementované do jedného zariadenia nazývaného SIP server. Jeho úlohou je smerovanie žiadostí o spojenie, realizácia doplnkových služieb, autentizácia a pod.

SIP je textovo orientovaný protokol s rysmi protokolov HTTP a SMTP: klient posiela žiadosti na server, ktorý zasiela odpovede podobne, ako HTTP protokol. V hlavičkách sa rovnako, ako v prípade SMTP komunikácie, nachádzajú položky From, To alebo Subject. Entita protokolu SIP je viazaná k doméne, ktorá je obsluhovaná SIP Proxy. Medzidoménová komunikácia prebieha medzi rôznymi SIP Proxy. SIP entity sú identifikované použitím menných identifikátorov SIP URI (Uniform Resource Identifier), ktorých všeobecný tvar je nasledujúci:

```
sip:user:password@host:port;uri-parameters?headers
```

Skladá sa teda z častí *username*, ktorá identifikuje užívateľa, *host*, vzťahujúca sa k doméne, z polí *password* (neodporúčané), *port* (štandardne UDP 5060) a prípadne ďalších parametrov. Väčšinou sa však SIP URI používa v jednoduchej podobe `sip:user@host`.

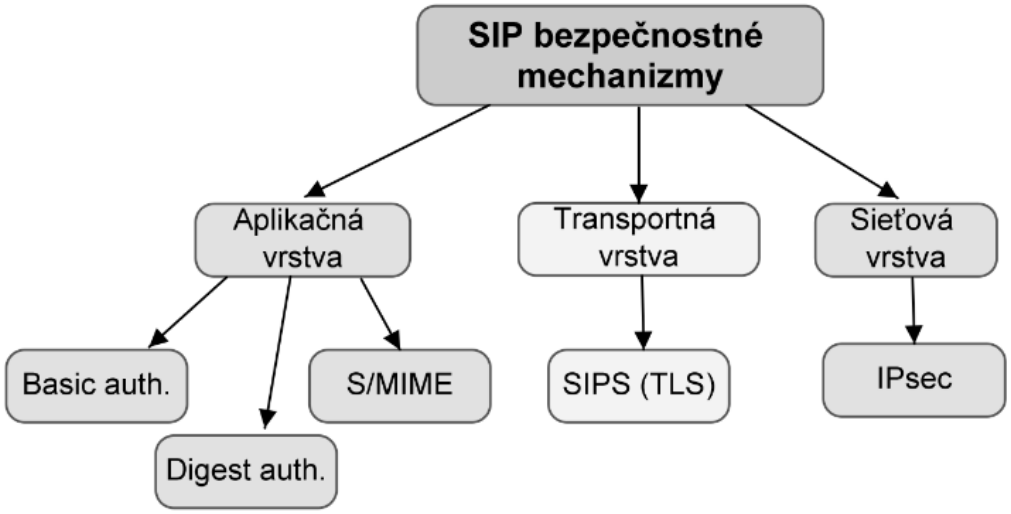


Obr. 1.4 Transakcia v SIP protokole.

Protokol SIP je sám o sebe nechránený, neobsahuje žiadne bezpečnostné ochrany. Z tohoto dôvodu boli definované bezpečnostné mechanizmy, ktoré sú v RFC 3261 definované nasledujúco:

- Zachovanie dôvery a integrity správ.
- Zabránenie replay útokom.
- Zamedzenie falšovania správ.
- Poskytnutie autentizácie a súkromia pre účastníkov komunikácie.
- Zabránenie útokom typu DoS.
- Zaistenie dôvery, integrity a autentizácie správ účastníkov.

Za najlepšiu techniku pre zachovanie dôvery v signalizácií je podľa RFC 3261 úplné šifrovanie správ. Vzhľadom na koncepciu protokolu SIP však nie je možné žiadosti a odpovede šifrovať v plnom rozsahu, keďže obsah polí, napríklad *Via* a *Route,* v hlavičke musí byt viditeľný pre proxy servery. Preto sa využívajú bezpečnostné mechanizmy na nižších vrstvách, viz. obrázok 1.5.



Obr. 1.5 Bezpečnostné mechanizmy protokolu SIP.

1.2.1 **Digest authentication**

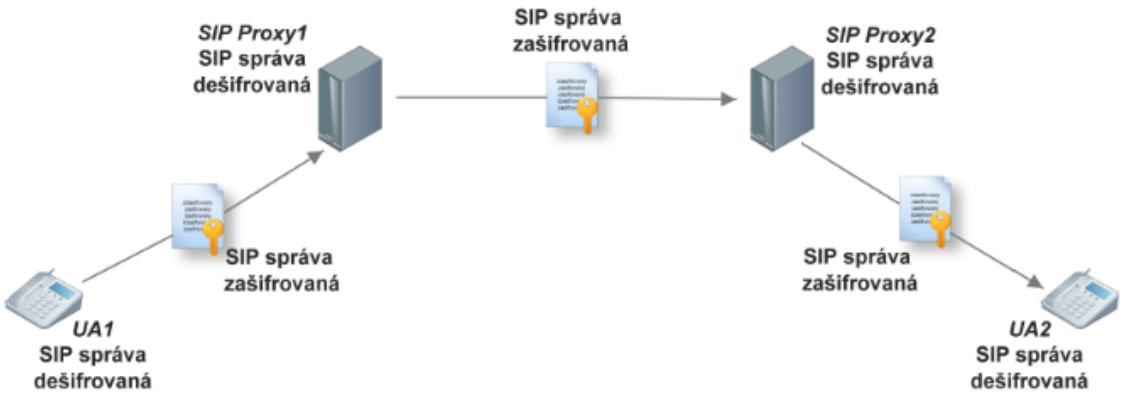
Digest Authentication je bezpečnostný mechanizmus, ktorý využíva staršiu metódu Basic Authentication, avšak namiesto prenosu overeného hesla ho šifruje pomocou hashovacej funkcie MD5. Tento mechanizmus je založený na SIP autentizačnej metóde vychádzajúcej z HTTP autentizácii. Princíp fungovania: ak je na server zaslaná koncovým užívateľom žiadosť REGISTER alebo INVITE, server túto žiadosť zamietne a pošle odpoveď. Tá obsahuje správu s informáciou, akým spôsobom má byť žiadosť autentizovaná. UA následne do hlavičky ďalšej žiadosti pridá pole s požadovanou autentizáciou. Takéto autentizačné pole môže obsahovať viac parametrov, napríklad typ šifrovacieho algoritmu, heslo, rozsah platnosti atď.

1.2.2 S/MIME

S/MIME (Secure Multipurpose Internet Mail Extensions) je bezpečnostné rozšírenie štandardu pre šifrovanie a podpis e-mailových správ MIME. S/MIME sa začalo využívať aj v protokole SIP, ktorého správy tiež môžu obsahovať telo MIME. Je tak možné šifrovať telá MIME správ v žiadostiach a odpovediach bez toho, aby boli ovplyvnené hlavičky správ. Telo správy sa podpisuje súkromným kľúčom odosielateľa a zašifrované verejným kľúčom príjemcu. Na to sa využívajú rôzne šifrovacie algoritmy, napríklad RSA, 3DES, AES a hashovacie algoritmy MD5 alebo SHA-1. Tým sa zaisťuje integrita a dôvera správ od volajúceho až k volanému.

1.2.3 SIPS

SIPS, alebo tiež SIP cez TLS (Transport Layer Security), je bezpečnostný mechanizmus prevzatý z HTTPS protokolu. Slúži pre hop-by-hop prenos SIP šifrovaných správ. TLS sa skladá z Handshake protokolu (vyjednávanie a koordinácia komunikačných parametrov) a Record protokolu (fragmentácia a kompresia datagramov, šifrovanie, hash). Princíp fungovania: SIP správa je šifrovaná na základe TLS scenára (medzi UAC a UAS je vyžadovaná výmena platných certifikátov, ktoré boli poskytnuté dôveryhodnou certifikačnou autoritou) a následne už môže byť komunikácia zabezpečená len hop-by-hop metódou. SIPS však zaručuje dôveryhodnosť a integritu SIP správ len medzi dvoma prvkami siete, nie na celej trase spojenia, ako je zobrazené na obrázku 1.6.



Obr. 1.6 SIPS.

1.2.4 IPsec

IPsec (Internet Protocol Security) je súbor mechanizmov a algoritmov, ktorého úlohou je zabezpečenie komunikácie na sieťovej vrstve OSI modelu. Tento protokol sa najčastejšie používa v architektúrach, kde má niekoľko užívateľov či celých domén už medzi sebou vytvorenú dôveru k ostatným účastníkom. Tento stav v sieti je tiež známy ako medzidoménová dôvera. IPsec je otvorený štandard popísaný v RFC 4301, a je jednou z najrozšírenejších VPN technológií. Na rozdiel od iných VPN technológií, IPsec spĺňa všetky požiadavky na kvalitnú sieť VPN. Tento protokol je tiež možné použiť pre hop-by-hop metódu, napríklad v prípade, kedy majú UA vymenené zdieľané kľúče so SIP Proxy vzdialenou iba jeden hop.

2 Bezpečnostné riziká v IP telefónii

V predchádzajúcej kapitole boli popísané bezpečnostné mechanizmy využívané v IP telefónii pre protokol SIP a RTP. Tieto zabezpečenia je nutné navrhovať, keďže spôsobov útoku na VoIP sieť je veľké množstvo a stále sa objavujú nové možnosti. VoIP je totižto službou pracujúcou v reálnom čase, takže dostatočne rýchle odhalenie a zabránenie útoku môže byť náročné. Vzhľadom na to, že SIP je textovo orientovaný protokol s rysmi HTTP, i bezpečnostné riziká sú pre tieto protokoly podobné. Riziko zneužitia sa zvyšuje aj tým, že infraštruktúra IP telefónie sa okrem telefónov a serverov skladá z rôznych podporných prvkov, u ktorých aj malá úprava nastavenia stačí na poškodenie siete. Táto kapitola je preto zameraná na možné bezpečnostné riziká v IP telefónii.

2.1 Monitoring a manipulácia so signalizáciou

Pomocou signalizačných správ sa nadväzuje, udržiava a ukončuje hovor. Zachytávaním signalizácie je možné odhaľovať aktívne zariadenia v sieti a zbierať potrebné informácie k ďalším útokom. Akoukoľvek zmenou signalizácie vo VoIP infraštruktúre môže útočník spôsobiť narušenie integrity hovoru. V tejto podkapitole uvediem príklady takýchto útokov:

Pri mapovaní čísel útočník zachytáva SIP žiadosti, ako napríklad INVITE, v ktorej sa nachádzajú čísla a mená použitých SIP účtov. Nazbierané informácie je možné využiť napríklad na následný SPAM, ktorý je aj v IP telefónii obľúbeným útokom. SIP žiadosť INVITE sa dá zneužiť aj na neželané presmerovanie toku dát. Stačí, aby narušiteľ v tejto metóde modifikoval adresu príjemcu na inú, než kam bola správa pôvodne smerovaná, napríklad na adresu svojho SIP telefónu.

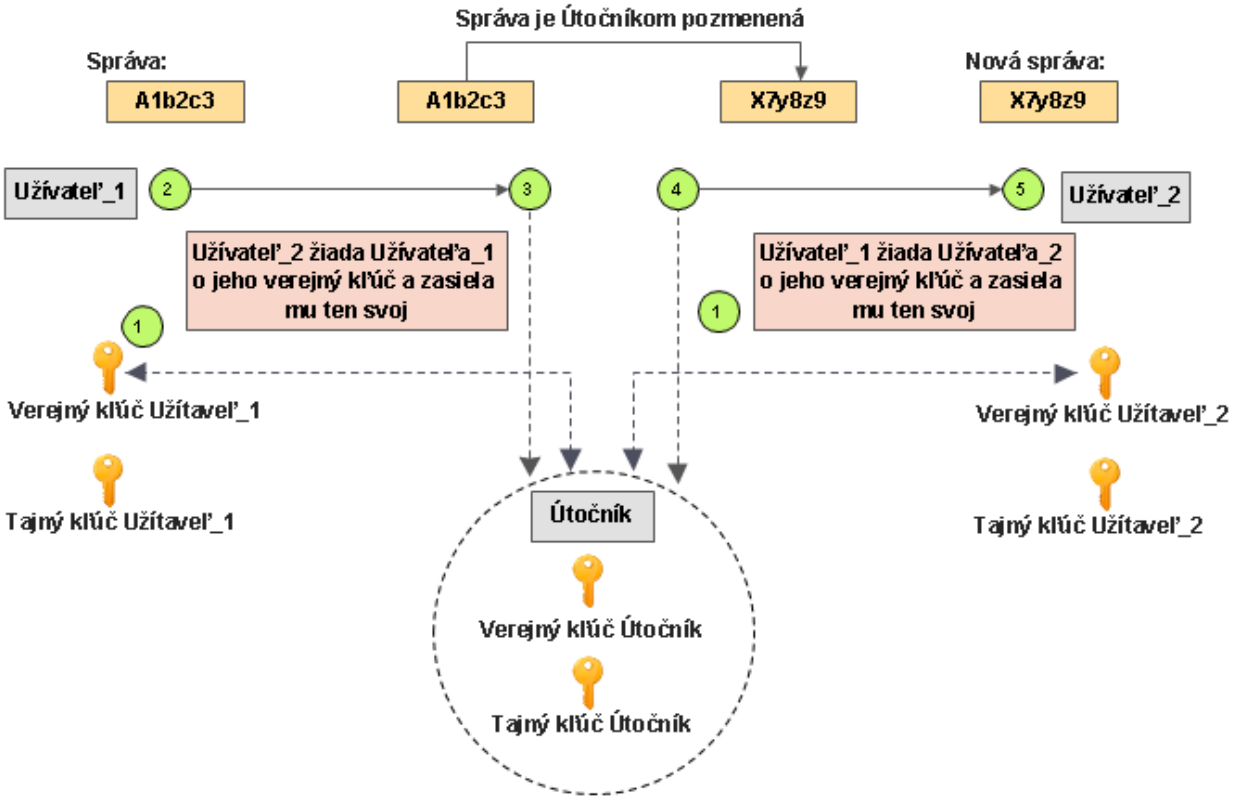
Odobranie registrácie je tiež veľmi jednoduchým, ale účinným spôsobom narušenia hovoru. Metódou REGISTER je na SIP server po zapnutí zaregistrované každé koncové zariadenie, pričom túto metódu následne opakovane zasiela, väčšinou v predvolenom intervale 3600 sekúnd. Vďaka tejto registrácií SIP server vie, kam majú byť smerované prichádzajúce hovory. Ak však útočník registráciu odstráni, koncové zariadenia nebudú schopné prichádzajúce hovory prijímať. Tak, ako je narušiteľ schopný SIP žiadosť REGISTER odobrať, môže ju aj priradzovať. A keďže je vo VoIP infraštruktúre založenej na protokole SIP možné priradenie viac kontaktov na jednu registráciu, útočníci túto vlastnosť v nezabezpečených sieťach zneužívajú. Znamená to totiž, že v prípade prichádzajúceho hovoru môže zvoniť súčasne viac IP telefónov v rôznych lokalitách. Narušiteľ tak po pridaní registrácie na adresu svojho SIP zariadenia môže hovor prijímať ako prvý.

Ďalším závažným a útočníkmi veľmi obľúbeným spôsobom narúšania VoIP infraštruktúry je skenovanie siete. Jedná sa o identifikáciu aktívnych zariadení na SIP pobočkovej ústredni pomocou SIP žiadostí INVITE, REGISTER či OPTIONS. Ak týmto spôsobom útočník narazí na existujúce SIP účty, môže následne útokmi hrubou silou či slovníkovou metódou účinne zistiť valídne heslá a získať tak k účtom neobmedzený prístup.

2.2 Man in the Middle

Man-in-the-Middle útok je typický tým, že sa útočník nachádza medzi dvoma účastníkmi, ktorí veria, že spolu navzájom komunikujú. Ich komunikácia je bez ich vedomia zachytávaná a tok dát menený podľa potrieb útočníka, viz. obrázok 2.1. Pri tomto spôsobe narušenia záleží aj na tom, kde presne sa útočník v sieti nachádza. Môže byť totižto umiestnený medzi SIP proxy a užívateľom, tváriť sa ako samotná SIP proxy, alebo sa nachádzať medzi užívateľom a jedným zo serverov poskytujúcich infraštruktúre VoIP doplnkové služby ako DNS, DHCP či TFTP.

Už z popisu útoku vyplýva, že spoliehať sa na bezpečnú výmenu verejného kľúča nie je možné, keďže útočník kľúče môže zachytávať a pozmeniť. Riešením tohoto problému môže byť overovanie kľúčov pomocou elektronického podpisu účastníkov s využitím certifikačnej autority. Pre protokol SRTP bola vyvinutá nadstavba ZRTP, ktorá obsahuje bezpečnostný nástroj odolný útoku Man-in-the-Middle.



Obr. 2.1 Útok Man in the Middle.

2.3 DoS útoky

DoS (Denial od Service), v preklade odmietnutie služby, je útok, pri ktorom sú internetové služby rôznymi formami tak zahlcované, že dôjde k ich nefunkčnosti. Znamená to, že tento útok užívateľom bráni zvolené služby využívať. Variantou DoS je DDoS (Distributed DoS), počas ktorého je vybraná služba zahlcovaná väčším množstvom počítačov naraz. Technológia VoIP je na DoS útok veľmi náchylná, keďže komunikácia prebieha v reálnom čase a aj menší útok môže spôsobiť nepoužiteľnosť služieb. V IP telefónii sa DoS útoky zameriavajú najmä na SIP a RTP protokoly.

DoS útok na SIP protokol môže byť veľký problém, keďže napadnutím signalizácie je možné ohroziť ktorúkoľvek časť VoIP siete. Najčastejším cieľom narušiteľov je SIP proxy server. V takýchto prípadoch sa dá účinne využiť záplavový (flood) útok, pomocou ktorého je vygenerované tak veľké množstvo žiadostí, až vyťažia server a následné nadviazanie hovoru nie je možné.

Záplavový DoS útok na signalizačný protokol SIP môže mať viac podôb, príkladom sú UDPflood či InviteFlood. V prípade UDPfloodu útočník zasiela veľké množstvo UDP paketov na cieľový server, ktorý sa preťaží. Je to jeden z najvyužívanejších DoS útokov, pretože obrana voči nemu je náročná. Podobne je tomu tak aj pri útoku InviteFlood, kedy je server zahltený SIP žiadosťami INVITE.

Vysoká efektivita záplavového DoS útoku sa potvrdila aj na transportných protokoloch, medzi ktoré môžeme zaradiť aj RTP protokol. Ten je vo VoIP technológii využívaný prakticky najviac. Z dôvodu prenášania dát v reálnom čase je RTP protokol na záplavové útoky veľmi citlivý. Cieľom sa často stávajú koncové IP telefóny, ktoré sú po útoku nepoužiteľné. Výsledný hovor sa stáva nekvalitným, alebo ho ani nie je možné nadviazať.

3 Nástroje pre implementáciu VoIP honeypotov

Pod pojmom honeypot sa v sieťovej bezpečnosti skrýva rada služieb, nástrojov a implementácií, ktoré sú zámerne vystavené riziku útoku. Ako už názov napovedá, jedná sa u druh lákadla pre narušiteľov siete. Honeypoty sú navrhované na odhaľovanie nedostatočného zabezpečenia a získavanie informácií o priebehu útoku. Tie bývajú následne používané na identifikovanie nových metód útokov a pre prevenciu incidentov. Honeypoty môžu byť takisto aj účelne vystavované útokom na odlákanie od dôležitých systémových zdrojov.

Navonok honeypot pôsobí ako reálny systém a na základe toho aj komunikuje s okolím. V tejto dobe je vyvíjaných mnoho honeypot riešení, ktoré napodobňujú rôzne služby. Delia sa do rôznych skupín na základe rôznych kritérií. Najčastejšie je možné sa stretnúť s delením podľa miery interakcie. Honeypoty s nízkou mierou interakcie emulujú len určitú službu. Čím je miera interakcie vyššia, tým sa honeypot viac podobá reálnemu systémovému zdroju. Najvyššiu mieru interakcie mávajú honeynety, čo sú celé siete honeypotov. Ďalej je možné honeypoty deliť aj podľa toho, či útočníka aktívne lákajú, alebo na útok len pasívne vyčkávajú. Do druhej z týchto možností patria napríklad tzv. serverové honeypoty. Kvôli stále sa rozvíjajúcim bezpečnostným hrozbám vznikla aj skupina klientských honeypotov. Z názvu je zjavné, že sa jedná o honeypot vydávajúci sa za klienta určitej služby. Príkladom môže byť emulátor webových prehliadačov, či honeypot simulujúci koncový bod v IP telefónii.

Honeypoty bývajú spravidla jednoducho rozšíriteľné nástroje schopné spolupracovať aj s inými bezpečnostnými prvkami v sieti. V nasledujúcich podkapitolách uvediem vybrané riešenia pre siete internetovej telefónie.

3.1 Artemisa

Artemisa je open-source klientský honeypot nasadzovaný vo VoIP sieťach na protokole SIP, umožňujúci odhaľovať nepriateľské aktivity už v ranom štádiu. Simuluje SIP UA-koncový bod ako napríklad IP telefón, a čaká na prichádzajúci útok. Pri prichádzajúcom hovore odpovedá nadviazaním relácie a zároveň skúma prijaté SIP správy. Analyzuje dáta obsiahnuté v správach, doménové adresy, SIP porty a stopy známych nástrojov používaných na útoky. Vďaka tomu je schopný takmer okamžite zistiť prítomnosť nepriateľských aktivít. Artemisa zachytené útoky klasifikuje do niekoľkých skupín, napríklad Skenovanie, SPIT (Spam Over Internet Telephony), Útočný Nástroj, Vyzváňanie, a iných. Detekuje DoS a DDoS záplavové útoky InviteFlood a OptionsFlood. Zároveň kontroluje prijaté RTP dáta a audio stopu, ktorú vo WAV formáte ukladá do vopred definovanej zložky. Po ukončení analýzy sa výsledné informácie zobrazujú v konzole honeypotu a ukladajú sa do textového dokumentu a HTML dokumentu. Je tiež možné v konfiguračnom súbore nastaviť zasielanie oznámení o útoku na zvolenú e-mailovú adresu.

Artemisa nemusí pôsobiť len ako klientský honeypot. Môže byť využívaná aj pre úpravu politík zabezpečenia domény, real-time nastavovanie firewallu, napríklad okamžité zakazovanie IP adries či ID volajúceho.

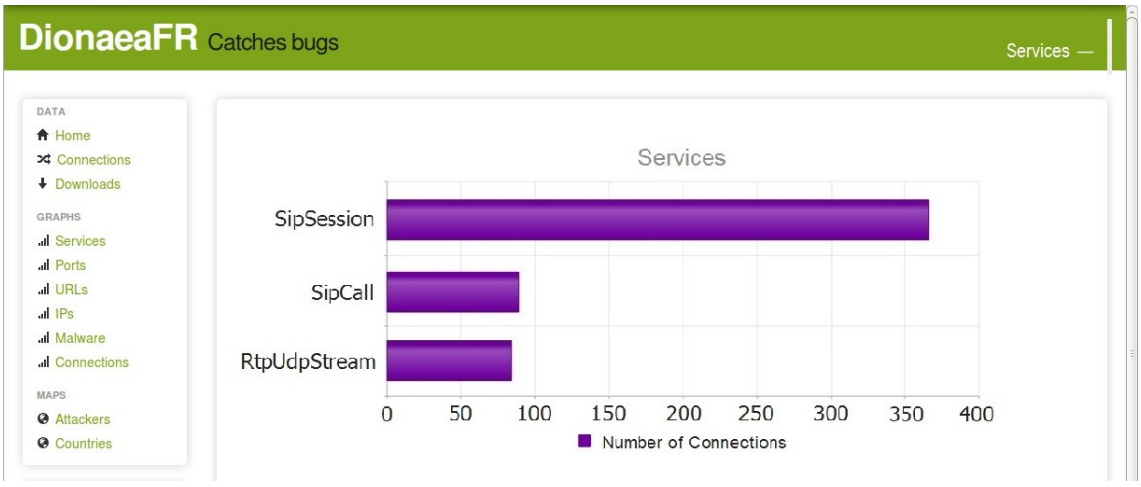
3.2 Dionaea

Dionaea je honeypot vyvinutý za účelom detekcie malware. Ten Dionaea zachytáva tým, že v sieti vystavuje vybrané simulované služby takmer nezabezpečené. Po zachytení útoku si celý malware skopíruje. Aby sa zamedzilo zneužitiu, pracuje v obmedzenom prostredí bez administratívnych práv. Jeho skriptovacím jazykom je Python, je schopný detekovať shellcode pomocou LibEmu, podporuje IPv6, TLS a operačný systém Linux. Stopy známych programov používaných na útoky rozpoznáva s využitím nástroja P0f. Po nadviazaní spojenia s útočníkom dokáže identifikovať spôsob jeho pripojenia do siete, použitý systém, jeho vzdialenosť, masquerading (prepis zdrojovej adresy) a iné.

Honeypot Dionaea je nástroj s nízkou mierou interakcie. Znamená to, že dokáže simulovať len určité sieťové služby:

- Hypertext Transfer Protocol (HTTP) – protokol pre výmenu hypertextových dokumentov. Okrem neho Dionaea podporuje tiež zabezpečený HTTPS
- File Transfer Protocol (FTP) – často napádaný protokol pre prenos súborov
- Server Message Block (SMB) – protokol slúžiaci na zdieľaný prístup k súborom a zariadeniam v sieti, ktorý je obľúbeným cieľom hackerov
- Microsoft SQL Server (MSSQL) – databázový systém vyvinutý Microsoftom
- Voice over IP (VoIP) – Dionaea pre túto službu využíva protokol SIP

V prípade simulácie služby VoIP Dionaea čaká na prichádzajúce SIP správy, na ktoré následne reaguje vytvorením relácie. Podporuje najvyužívanejšie SIP žiadosti, prijíma RTP dáta a audio stopu, ktorú môže nahrávať. Zachytené informácie ukladá do textového dokumentu alebo do SQLite databázy. Pre prehľadnú analýzu detekovaných aktivít bol vytvorený nástroj DionaeaFR. Ten zobrazuje zoznam všetkých útokov, štatistické grafy (viz. obr. 3.1), zdrojové IP adresy, mapu zobrazujúcu odkiaľ útok pochádza a mnoho ďalších prakticky spracovaných informácií.



Obr. 3.1 Nástroj DionaeaFR.

3.3 Tcpdump

Nástroj Tcpdump sa typicky neradí medzi honeypoty, je však nutné sa s ním zoznámiť pre bližšie pochopenie nasledujúcich kapitol.

Tcpdump je jedným zo základných paketových analyzérov. Dokáže zachytávať a zobrazovať všetky pakety odosielané cez sieťové rozhranie. Je využívaný na analyzovanie komunikácie v sieti s rôznymi protokolmi pre jeho veľké množstvo funkcií. Je distribuovaný pod BSD licenciou, čo umožňuje jeho voľné šírenie. Tcpdump podporuje väčšinu Unixových operačných systémov, pričom pre zachytávanie paketov využíva knižnicu libpcap. Bola tiež vyvinutá verzia pre operačný systém Windows pod názvom WinDump.

Tcpdump pracuje v príkazovom riadku. Po spustení zachytáva každý paket, ktorý prechádza cez daný sieťový port. Na vyťažených serveroch však môže byť táto vlastnosť nežiadúca. Z tohoto dôvodu Tcpdump podporuje veľké množstvo filtrov. Filtrovanie zachytávaných paketov tak môže byť založené napríklad na základe vybranej IP adresy, konkrétneho portu, počtu paketov, typu protokolu (TCP/UDP/ICMP) a iných kritérií.

Tento nástroj je tiež účinný pri zachytávaní VoIP SIP paketov. Stačí si vyfiltrovať IP telefóniou využívaný UDP protokol, či port 5060, ktorý používa SIP protokol. Takto zachytené pakety je možné ukladať do súborov vo formáte .pcap, ktoré sa dajú následne spustiť napríklad v programe Wireshark. Ten ponúka grafické užívateľské rozhranie s možnosťou prehľadných operácií so zachytenými paketmi, vrátane grafov zobrazujúcich transakciu v SIP protokole.

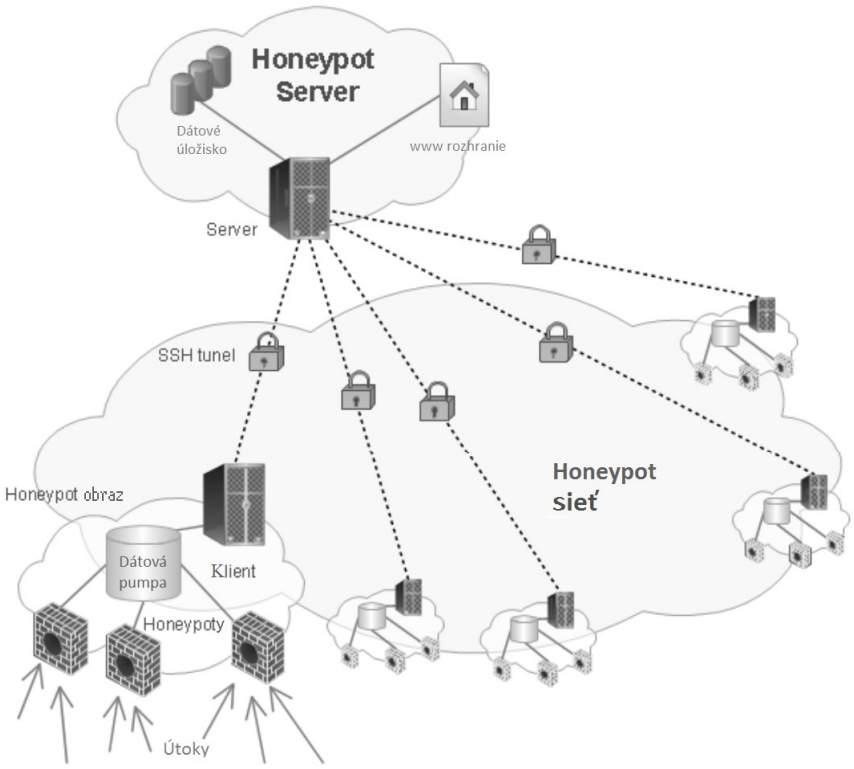
4 Podklady meraní a štatistika útokov

Cieľom tejto diplomovej práce je analýza dát z VoIP honeypotov, ktoré boli nasadené v sieti v reálnom prostredí a slúžili ako monitorovacie prostredie pre prichádzajúce útoky. Získavanie dostatočného objemu dát pre ich objektívnu analýzu je však časovo nad rámec diplomovej práce. Z tohoto dôvodu využívam dáta, ktoré mi poskytol Ing. Jakub Šafařík, získané pre jeho dizertačnú prácu [16] a výsledky tejto diplomovej práce budú následne využívané Ing. Šafaříkom v jeho práci.

Ing. Jakub Šafařík v tézach svojej dizertačnej práce [16] vytvoril distribuovaný systém sond, ktorý slúži pre zber informácií o útokoch na VoIP SIP infraštruktúru. Systém sa skladá zo sond typu honeypot Dionaea a analyzér Tcpdump. Tieto sondy sú umiestnené v rôznych sieťach oddelených logicky na úrovni topológie, aj geograficky, viz. obrázok 4.1. To umožňuje získať variabilné dáta o SIP útokoch v rôznych infraštruktúrach. Spracovanie získaných dát má na starosti centralizovaný server, ktorého modulom je algoritmus neurónovej siete [15]. Jeho hlavnou úlohou je zber, uchovávanie a analýza dát z jednotlivých sond.

Neurónová sieť je algoritmus, ktorého činnosť sa inšpiruje činnosťou ľudského mozgu. Je tvorený veľkým množstvom vzájomne prepletených buniek – neurónov, ktoré spolu komunikujú. Model neurónu sa skladá z troch častí (vstupná, výstupná a funkčná časť). Jednotlivé neuróny sú prepojované spojmi, ktoré sú ohodnotené váhami. Prepájajú sa medzi sebou do väčších štruktúr a usporadúvajú sa do vrstiev. Jednou z hlavných vlastností neurónovej siete je schopnosť učiť sa. V tejto súvislosti sa dátový súbor pre neurónovú sieť delí na trénovaciu množinu, testovaciu množinu a validačnú množinu. Cieľom učenia je nastavenie siete tak, aby dávala presné výsledky. Využívajú sa dva typy učenia, a to učenie s učiteľom a učenie bez učiteľa. Existuje celá rada neurónových sietí, pričom najjednoduchším modelom je Perceptron, ktorý pozostáva len z jediného neurónu. Neurónové siete majú široký rozsah využitia, okrem analýzy je možné ich využívať tiež na detekciu porúch strojov, v lekárstve, v doprave, na rozpoznávanie tváre, textu a iných.

Vo svojej práci Ing. Šafařík využíva neurónovú sieť typu MLP (Multi Layer Perceptron – Viacvrstvá perceptrónová sieť). Ako zdroj pre trénovaciu množinu boli použité dáta zo skutočných útokov, ktoré honeypot zachytával po dobu dvoch mesiacov. Neurónová sieť získané dáta klasifikuje do ôsmich tried. Trénovacia množia má v dobe tvorby tejto diplomovej práce 104 položiek, tj. 13 pre každú triedu. Aby sa zvýšila dôveryhodnosť klasifikovaných dát, využíva sa viac mechanizmov. Predpokladá sa, že ak by časť z nich vykazovala chybu, systém ako celok môže stále dosiahnuť správny výsledok. Pre overenie tohoto predpokladu budú slúžiť výsledky mojej diplomovej práce.



Obr. 4.1 Koncept distribuovanej siete honeypotov, autor Ing. J. Šafařík [16].

4.1 Získané dáta

Ako bolo už spomenuté v úvode tejto kapitoly, dáta sú neurónovou sieťou analyzované a klasifikované do niekoľkých kategórií. Klasifikácia prebieha na základe viacerých kritérií, napríklad podľa SIP žiadostí zachytených sondou počas útoku.

V tejto diplomovej práci analyzujem dáta, ktoré pochádzajú z výstupu neurónovej siete, sú teda roztriedené a klasifikované. Boli tiež prevedené do tabuľky Microsoft Office Excel, ktorá je k tejto práci priložená v prílohe. Ukážka takto spracovaných dát je na obrázku 4.2.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	id	sourc	ip	port	transpc	connec	regCour	invCour	ackCou	byeCo	canCou	optCou	subCou	connectior	connectionR	started	delta	result	countr
2	9762	1	142.54.18	5074	udp	2	0	1	0	0	0	0	0	0.5	48289	1.7.2015 0:04	1	call_test	US
3	9763	1	142.54.18	5074	udp	2	0	1	0	0	0	0	0	0.5	48295	1.7.2015 0:14	1	call_test	US
4	9764	1	142.54.18	5074	udp	2	0	1	0	0	0	0	0	0.5	48301	1.7.2015 0:23	1	call_test	US
5	9765	1	142.54.18	5074	udp	2	0	1	0	0	0	0	0	0.5	48307	1.7.2015 0:33	1	call_test	US
6	9766	1	142.54.18	5074	udp	3	0	1	0	0	0	0	0	0.333333	48311	1.7.2015 0:42	10	call_test	US
7	9767	1	142.54.18	5076	udp	2	0	1	0	0	0	0	0	0.5	48316	1.7.2015 0:52	1	call_test	US
8	9768	1	173.224.1	5078	udp	2	0	1	0	0	0	0	0	0.5	48293	1.7.2015 0:11	1	call_test	US
9	9769	1	192.99.67	5076	udp	2	0	1	0	0	0	0	0	0.5	48297	1.7.2015 0:21	0	call_test	CA
10	9770	1	192.99.67	5078	udp	2	0	1	0	0	0	0	0	0.5	48318	1.7.2015 0:55	1	call_test	CA
11	9771	1	192.99.69	5070	udp	2	0	1	0	0	0	0	0	0.5	48291	1.7.2015 0:10	1	call_test	CA
12	9772	1	192.99.69	5071	udp	2	0	1	0	0	0	0	0	0.5	48299	1.7.2015 0:21	1	call_test	CA
13	9773	1	192.99.69	5071	udp	2	0	1	0	0	0	0	0	0.5	48309	1.7.2015 0:33	1	call_test	CA
14	9774	1	192.99.69	5073	udp	2	0	1	0	0	0	0	0	0.5	48314	1.7.2015 0:44	0	call_test	CA
15	9775	1	192.99.69	5074	udp	2	0	1	0	0	0	0	0	0.5	48320	1.7.2015 0:56	2	call_test	CA
16	9776	1	195.154.1	5070	udp	2	0	1	0	0	0	0	0	0.5	48303	1.7.2015 0:31	1	call_test	FR
17	9777	1	37.220.7.2	5071	udp	2	0	1	0	0	0	0	0	0.5	48305	1.7.2015 0:33	1	call_test	GB

Obr. 4.2 Ukážka analyzovaných dát vo forme tabuľky Excel.

Dáta spracované neurónovou sieťou poskytujú o každom zachytenom útoku veľké množstvo informácií. Každému útoku je pridelené identifikačné číslo „ID“. V stĺpci „Source“ sa nachádza zdrojová sonda, pričom pod číslami 1 a 3 sa nachádzajú sondy typu Dionaea, pod číslami 4 a 5 sú Tcpdump sondy. Uvádza sa tiež IP adresa, z ktorej bol útok iniciovaný, číslo portu, a tiež typ transportného protokolu a počet pripojení. V nasledujúcich stĺpcoch sú uvedené súčty jednotlivých SIP žiadostí využívaných útočníkom počas jednotlivých útokov. Týmito SIP žiadosťami sú REGISTER, INVITE, ACK, BYE, CANCEL, OPTIONS, SUBSCRIBE. V stĺpci „Result“ sa nachádza typ útoku, ktorý algoritmus neurónovej siete vyhodnotil na základe sledovaných veličín. Útoky môžu byť vyhodnotené nasledovne:

- call_test – útočník sa pokúšal o volanie cez danú PBX, detekcia pomocou INVITE SIP správ
- opt_scan – skenovanie serveru pomocou vyššieho počtu správ OPTIONS
- opt_test – skenovanie serveru pomocou nižšieho počtu správ OPTIONS
- reg&call – útočník sa pokúšal o registráciu a nadviazanie hovoru za využitia SIP správ REGISTER a INVITE
- reg_attempt – pokus o legitímnu registráciu či jednoduchý test registrácie
- reg_test – útočník sa pokúšal o získanie registrácie na danom serveri pomocou vyššieho počtu SIP správ REGISTER
- reg_test_high – útok zahlcovaním alebo DoS útok s využitím SIP správ REGISTER na daný stroj
- ukwSIP/noSIP – jedná sa o neznámy útok pomocou ďalších možných SIP správ (iné než RFC 3261) / útok, ktorý bol smerovaný na SIP port, no neobsahuje SIP správy

Z tejto tabuľky je tiež možné sa dozvedieť presný čas a dátum, v ktorý sonda začala útok zachytávať, doba trvania útoku v sekundách, ako aj názov štátu, oblasti a konkrétneho mesta, z ktorého bol útok iniciovaný.

4.2 Spôsob spracovávania dát

Táto podkapitola je venovaná detailnému popisu techník, ktoré budú využívané pri spracovávaní poskytnutých dát. Zachytené dáta sa dajú analyzovať rôznymi spôsobmi podľa toho, aké informácie sa potrebujeme dozvedieť. V prípade tejto diplomovej práce sa spôsob spracovávania poskytnutých dát odrážal od potreby požiadavkov vychádzajúcich z bezpečnostných analýz a popularity jednotlivých typov použitých útokov.

V tejto práci mám k dispozícii dáta zo sond typu Dionaea s identifikačnými číslami 1 a 3, a sond typu Tcpdump s identifikačnými číslami 4 a 5. Všetky techniky využívané pre spracovávanie dát budú najskôr overené na testovacej sade dát. Jedná sa o približne 8500 sondami zachytených útokov počas 15tich dní.

4.2.1 **Porovnávanie počtu zachytených útokov**

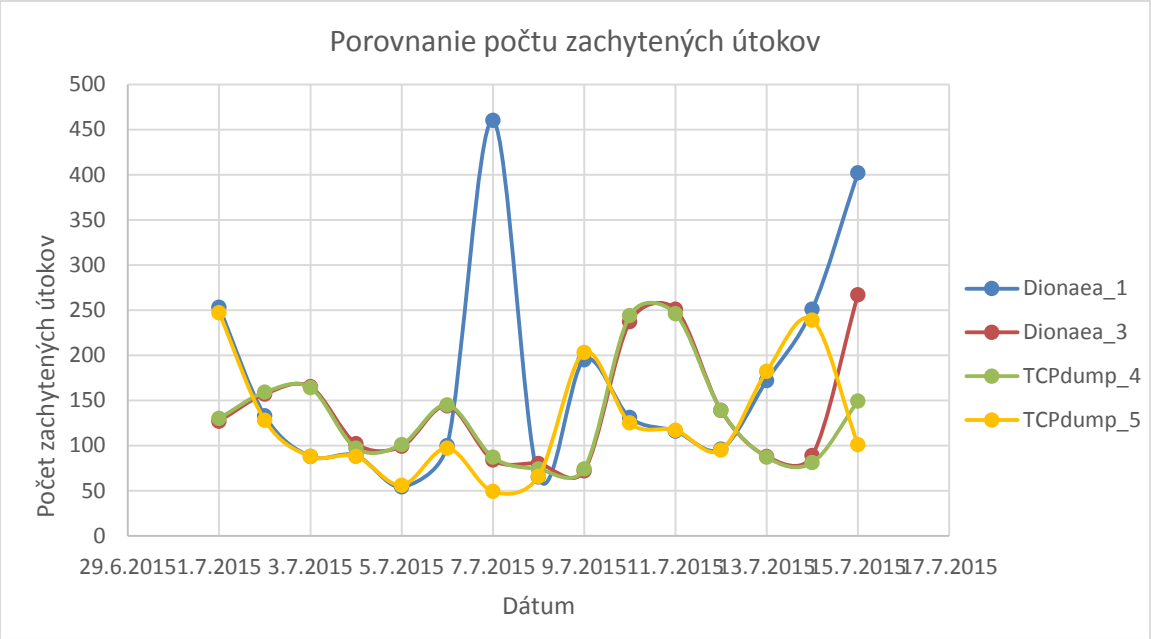
Na úvod analýzy dát je nutné najskôr zistiť, koľko útokov bolo sondami zachytených v rámci určitého časového obdobia. Predpokladá sa, že sonda Dionaea_1 zachytáva rovnaké množstvo útokov ako sonda Tcpdump_5, a sonda Dionaea_3 zachytáva rovnaké množstvo útokov ako sonda Tcpdump_4.

Keďže cieľom práce je analyzovať dáta zachytávané niekoľko mesiacov, zvolila som pre detailnú a prehľadnú analýzu porovnávanie počtu útokov zachytených v rámci jedného dňa. Ak by sme však napríklad chceli analyzovať dáta zachytávané niekoľko rokov, bolo by vhodnejšie porovnávanie počtu útokov zachytených v rámci jedného mesiaca (porovnávanie v období jedného dňa by v takomto prípade bolo zbytočne detailné a neprehľadné).

Táto metóda bola overená na testovacej sade dát z útokov zachytávaných počas 15tich dní, viz. tabuľka 1. Na grafe 1 je vidieť, že vyššie spomínaný predpoklad bol splnený: Dionaea_1 zachytáva rovnaké množstvo útokov ako sonda Tcpdump_5, tak isto ako sonda Dionaea_3, ktorá zachytáva rovnaké množstvo útokov ako sonda Tcpdump_4. Výnimkou je len deň 7.7.2015, kedy došlo k poruche sondy Dionaea_1. Z tohoto dôvodu sa javí, akoby zachytila oproti iným dňom veľké množstvo útokov.

Dátum	Dionaea		Tcpdump	
	1	3	4	5
1.7.2015	253	127	130	247
2.7.2015	133	157	159	128
3.7.2015	88	165	164	88
4.7.2015	89	102	97	88
5.7.2015	54	99	101	56
6.7.2015	100	144	145	97
7.7.2015	460	84	87	49
8.7.2015	65	80	74	66
9.7.2015	195	72	74	203
10.7.2015	131	237	244	125
11.7.2015	116	251	246	117
12.7.2015	96	139	139	95
13.7.2015	172	88	87	182
14.7.2015	251	89	81	239
15.7.2015	402	267	149	101

Tab. 1 Počet zachytených útokov-testovacia sada dát.



Obr. 4.3 Porovnanie počtu zachytených útokov - testovacia sada dát.

4.2.2 Porovnávanie útokov na základe krajiny pôvodu – počet útokov

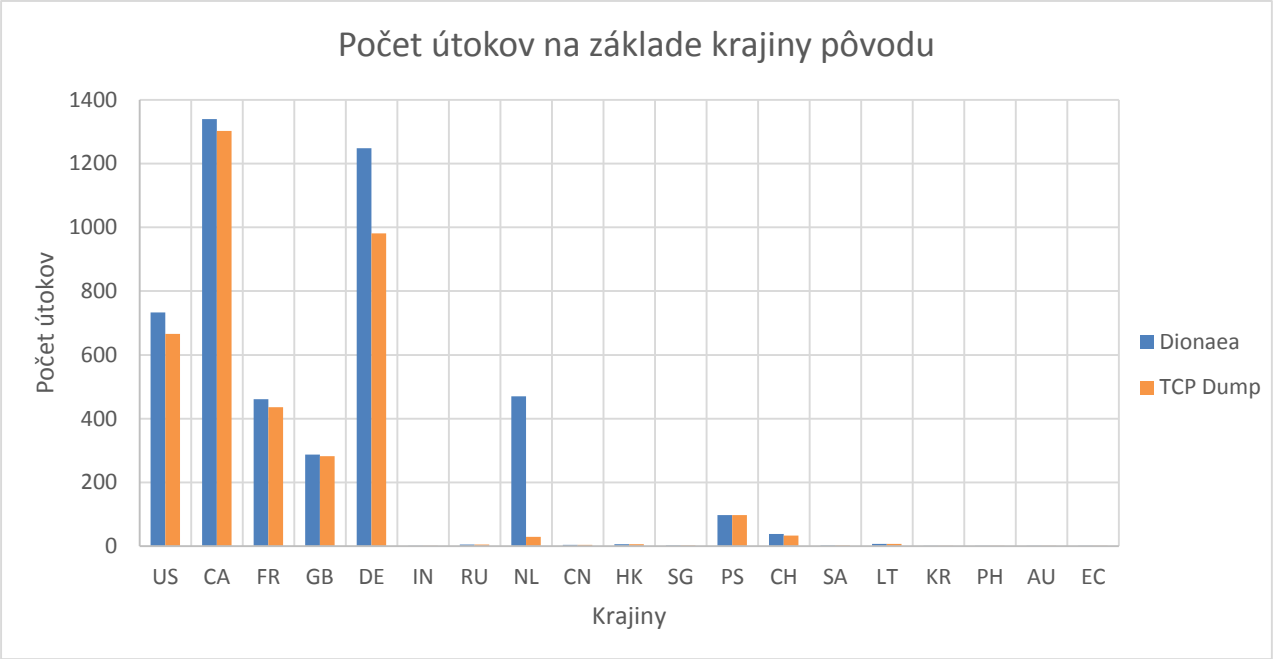
Pre dôkladnú analýzu zachytených útokov je nutné vedieť, z ktorých krajín prichádza najviac útokov. Predpokladá sa, že sondy typu Dionaea i Tcpdump budú vyhodnocovať krajiny pôvodu zhodne.

Tento predpoklad bol najskôr overený na testovacej sade dát z útokov zachytávaných počas 15tich dní, viz. tabuľka 2. Na grafe 2 je vidieť, že odchýlky medzi uvedenými krajinami sú len minimálne, najväčšia sa objavuje v prípade Holandska (NL), kedy Dionaea z tejto krajiny zachytila 470 útokov a Tcpdump len 29 útokov. Môže sa jednať o ojedinelý prípad z dôvodu poruchy sondy.

Dionaea									
US	**CA**	**FR**	**GB**	**DE**	**IN**	**RU**	**NL**	**CN**	**HK**
733	1340	461	287	1248	1	5	470	4	6
SG	**PS**	**CH**	**SA**	**LT**	**KR**	**PH**	**AU**	**EC**	
2	97	38	2	7	1	1	1	1	

Tcpdump									
US	**CA**	**FR**	**GB**	**DE**	**IN**	**RU**	**NL**	**CN**	**HK**
666	1302	436	282	981	1	5	29	4	6
SG	**PS**	**CH**	**SA**	**LT**	**KR**	**PH**	**AU**	**EC**	
2	97	33	2	7	1	1	1	1	

Tab. 2 Počet útokov na základe krajín - testovacia sada dát.



Obr. 4.4 Porovnanie počtu útokov na základe krajín - testovacia sada dát.

Vysvetlivky:

US – Spojené štáty Americké, CA – Kanada, FR – Francúzsko, GB – Veľká Británia, DE – Nemecko, IN – India, RU - Rusko, NL – Holandsko, CN – Čína, HK – Hong Kong, SG – Singapur, PS – Palestína, CH – Švajčiarsko, SA – Saudská Arábia, LT – Litva, KR – Kórea, PH – Filipíny, AU – Austrália, EC – Ekvádor, BE – Belgicko, BO – Bolívia, BR – Brazília, CZ – Česká Republika, EG – Egypt, IE – Írsko, IR – Irán, IS – Island, KG – Kyrgyzstán, LU – Luxembursko, MX – Mexiko, NG – Nigéria, NZ – Nový Zéland, PA – Panama, PH – Filipíny, PL – Polsko, QA – Katar, RO – Rumunsko, SE – Švédsko, TW – Taiwan, UA – Ukraina, VE – Venezuela, VN – Vietnam

4.2.3 **Porovnávanie útokov na základe krajiny pôvodu – typ útokov**

Pre vývoj bezpečnostných protiopatrení môže byť dôležité vedieť, aké typy útokov z daných krajín pochádzajú. V tejto analýze sa zameriam na top 5 krajín, z ktorých prichádzalo najviac útokov. Rovnako ako v predošlom príklade sa predpokladá, že sondy typu Dionaea i Tcpdump budú zachytávať zhodné informácie, z ktorých následne neurónová sieť vyhodnotí zhodný typ útokov.

Tento predpoklad bol najskôr overený na testovacej sade dát z útokov zachytávaných počas 15tich dní, viz. tabuľka 3. Krajinami, z ktorých prichádzalo najviac útokov sú v poradí Kanada, Nemecko, USA, Francúzsko a Veľká Británia. Na grafoch 3 až 7 je vidieť, že odchýlky medzi zachytenými útokmi sú len minimálne.

CA								
Dionaea	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	1318	2	20	0	0	0	0	0
Tcpdump	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	1299	2	0	0	0	1	0	0

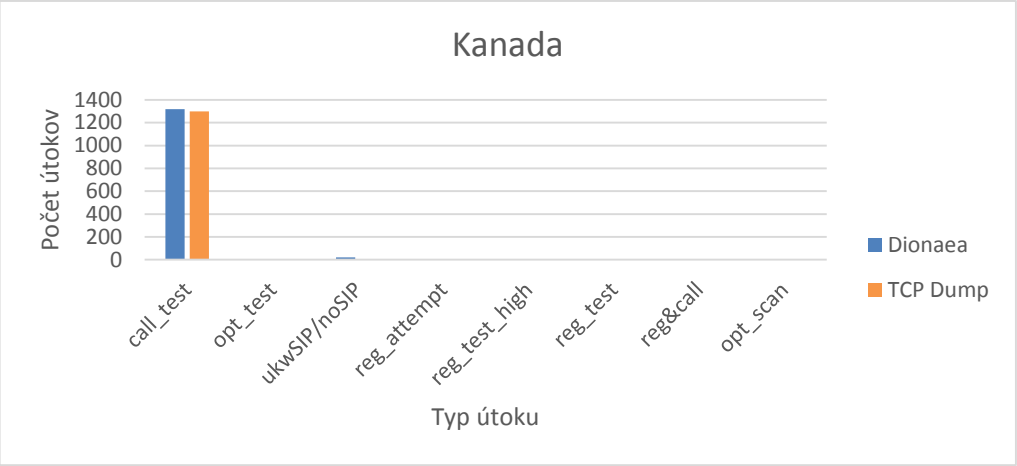
DE								
Dionaea	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	982	229	20	0	9	2	1	5
Tcpdump	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	734	234	6	1	2	3	1	0

US								
Dionaea	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	489	217	21	0	1	0	0	5
Tcpdump	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	450	210	5	0	1	0	0	0

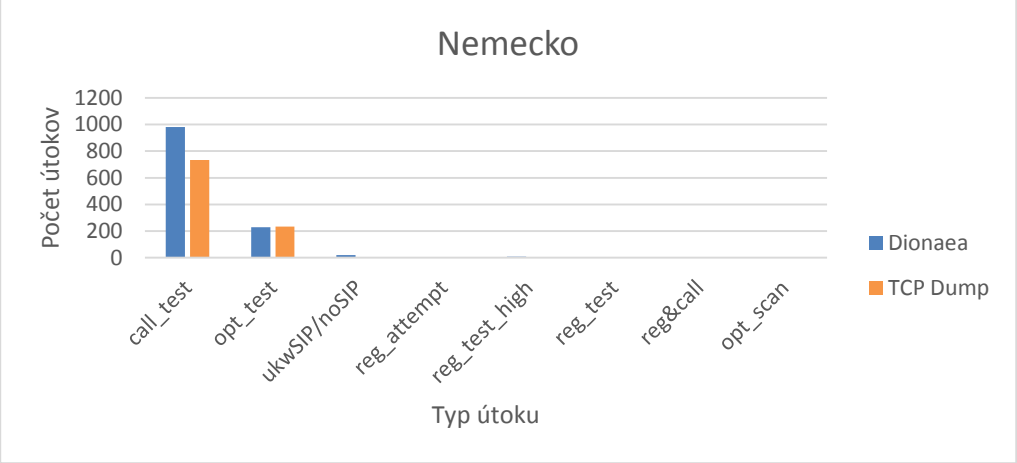
FR								
Dionaea	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	370	91	0	0	0	0	0	0
Tcpdump	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	348	84	0	0	0	4	0	0

GB								
Dionaea	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	256	9	3	0	0	0	19	0
Tcpdump	call_test	opt_test	ukwSIP/noSIP	reg_attempt	reg_test_high	reg_test	reg&call	opt_scan
	257	9	5	1	0	0	10	0

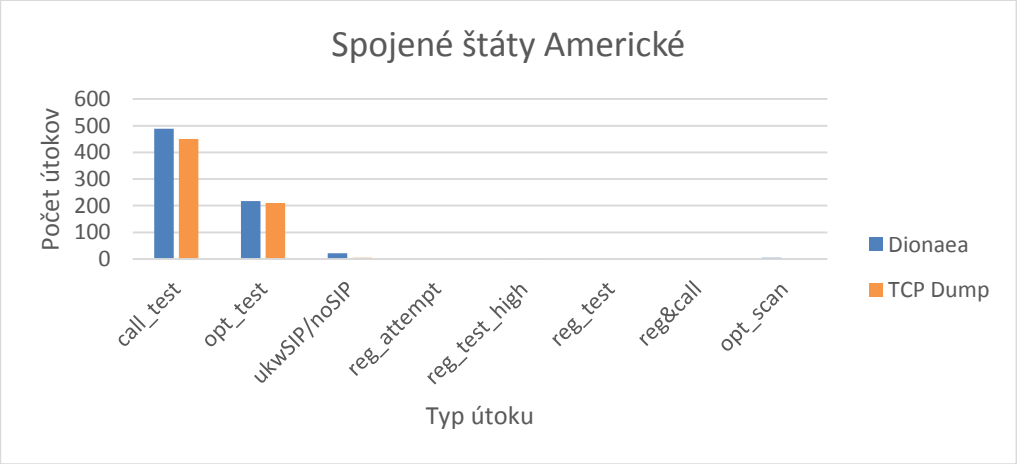
Tab. 3 Porovnanie typu útokov na základe krajín - testovacia sada dát.



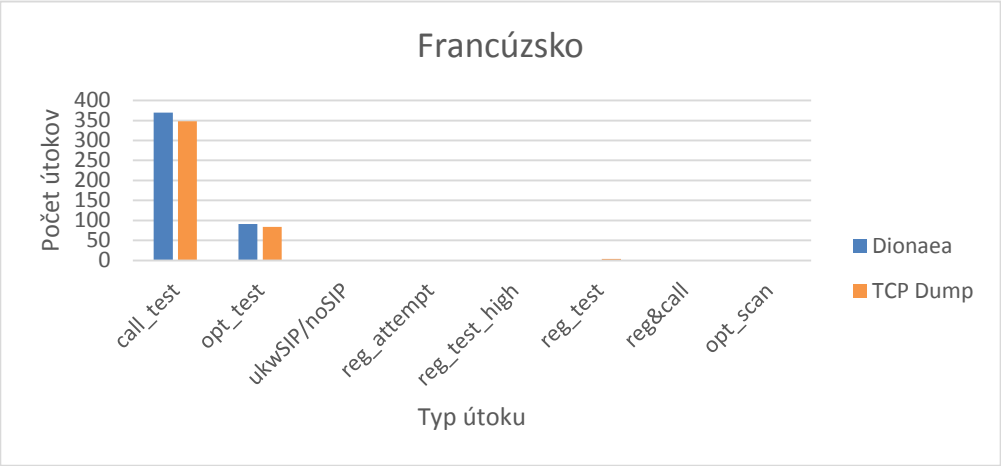
Obr. 4.5 Kanada, typ útokov - testovacia sada dát.



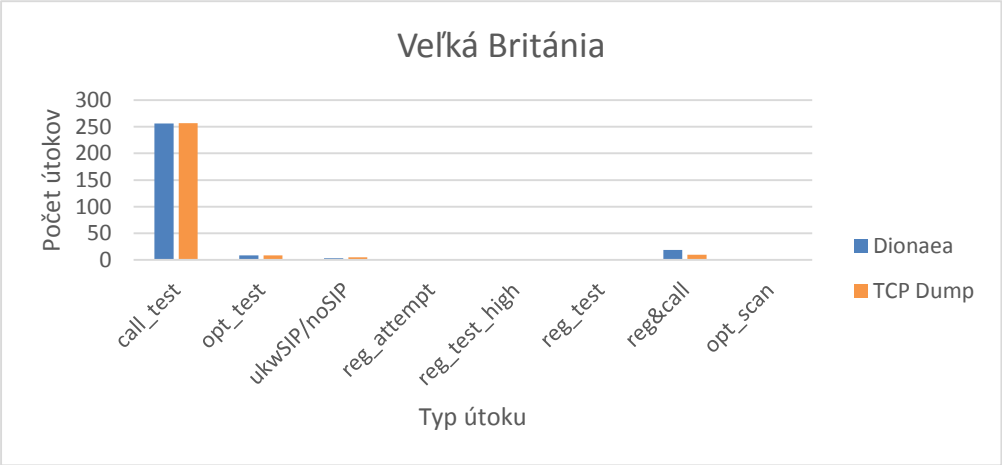
Obr. 4.6 Nemecko, typ útokov – testovacia sada dát.



Obr. 4.7 USA, typ útokov – testovacia sada dát.



Obr. 4.8 Francúzsko, typ útokov - testovacia sada dát.



Obr. 4.9 Veľká Británia, typ útokov - testovacia sada dát.

4.2.4 Najvyužívnejší druh útoku (testovacia sada dát)

Jedným z hlavných cieľov tejto diplomovej práce je vyhodnotenie, ktorý druh útoku je hackermi najvyužívanejší. Táto informácia je pri vytváraní bezpečnostných mechanizmov vo všeobecnosti veľmi dôležitá.

V tabuľke 4 je vidieť, že v testovacej sade dát, tj. 8565 zachytených útokov, je až 7253 z nich typu call_test. 1143 útokov je typu opt_test a len 89 útokov bolo vyhodnotených ako uknwSIP/noSIP. Ostatné typy útokov sa dajú považovať takmer zanedbateľné. Toto zistenie je prehľadne zobrazené na grafe 8.

Typ útoku	Počet	Percent [%]
call_test	7253	84,67
opt_scan	10	0,12
opt_test	1143	13,35
reg&call	31	0,36
reg_attempt	6	0,07
reg_test	10	0,12
reg_test_high	23	0,27
uknwSIP/noSIP	89	1,04
Celkom útokov	*8565*	*100*

Tab. 4 Využívanosť útokov – testovacia sada dát.

Obr. 4.10 Využívanosť útokov – testovacia sada dát.

4.2.5 **Opakované používanie zdrojových IP adries**

Pri zabezpečovaní siete je tiež dôležité vedieť, či útočníci využívajú zdrojové IP adresy jednorazovo, alebo sa k nim časom opakovane vracajú. Získame tak odpoveď napríklad na to, či sa oplatí automaticky blokovať adresy, z ktorých útoky prichádzajú, alebo je takéto zabezpečenie zbytočné.

Táto informácia bola najskôr zisťovaná na testovacej sade dát. Teoreticky by sa v nej malo nachádzať približne 4300 rôznych IP adries. Ukázalo sa, že väčšina IP adries je využívaná na 1-3 útoky len v jeden deň, prípadne na 1 útok trvajúci hodiny až niekoľko dní. V tabuľke 5 je ale vidieť, že niekoľko útočníkov svoje zdrojové IP adresy využíva opakovane na rovnaký typ útoku. V tabuľke 6 sa nachádzajú skupiny IP adries pochádzajúcich z rovnakej siete, ktoré boli na útočenie využívane v rovnaký čas na rovnaký typ útoku. V tomto prípade sa pravdepodobne jednalo o DDoS útok, tj. DoS útok z väčšieho množstva počítačov.

IP adresa	Dátum	Typ útoku	Krajina	
209.58.130.183	2.7., 3.7., 4.7., 5.7., 6.7., 7.7., 8.7., 10.7., 11.7., 12.7., 13.7., 14.7., 15.7.	opt_test	US	Virginia
212.83.134.85	1.7., 2.7., 3.7., 5.7., 6.7., 7.7., 9.7., 10.7., 11.7., 12.7., 13.7., 14.7., 15.7.	opt_test	FR	France
178.162.214.34	2.7., 6.7., 7.7., 8.7., 9.7., 10.7., 12.7., 14.7., 15.7.	opt_test, opt_scan	DE	Germany
188.138.1.239	4.7., 5.7., 8.7., 9.7., 10.7., 11.7., 14.7., 15.7.	opt_test, ukwSIP/noSIP	DE	Germany
195.154.181.206	2.7., 7.7., 8.7., 10.7., 11.7., 12.7., 15.7.	opt_test	FR	France
142.54.180.42	3.7., 4.7., 5.7., 7.7., 8.7., 9.7.	opt_test	US	Missouri
195.154.182.229	2.7., 9.7., 13.7., 14.7.	call_test	FR	France
194.63.142.86	1.7., 8.7., 10.7., 11.7.	opt_test	RU	Russia
95.211.156.155	8.7., 9.7., 15.7.	call_test	NL	Netherlands
107.150.43.170	5.7., 6.7., 9.7.	call_test	US	Missouri

Tab. 5 Opakované používanie IP adries – testovacia sada dát.

IP adresa	Dátum	Typ útoku	Krajina	
192.99.66.51 až 192.99.69.165	3.7., 4.7., 5.7., 6.7., 9.7., 10.7., 11.7.,12.7., 13.7., 14.7.	call_test, ukwSIP/noSIP	CA	Quebec
199.217.115.21 až 199.217.117.85	1.7. - 15.7.	opt_test	US	Missouri

Tab. 6 IP adresy rovnakej siete – testovacia sada dát.

4.2.6 Štatistická analýza dát

Pre analýzu budú využívané software QtiPlot [31] a GraphPad Prism [32]. Celý súbor analyzovaných dát sa nachádza v tabuľke I: Počet zachytených útokov jednotlivými sondami, viz. Príloha A a v tabuľke II: Porovnanie zachytených útokov Dionaea vs Tcpdump. Analyzovaných bude 122 záznamov zo sond typu Dionaea a typu Tcpdump a tiež z každej sondy zvlášť. Ukážka dát sa nachádza na obrázku 4.2.

Najskôr budú vytvorené krabicové grafy pre demonštráciu prípadných rozdielov medzi sondami. Na prvý pohľad by tak mal byť zrejmý prípadný odstup v množstve zachytávaných útokov. To, či sú rozdiely medzi sondami štatisticky významné, bude potvrdené v ďalších testoch. Shapiro-Wilkovým testom bude overená normalita dát. Následne bude overená rozdielnosť súborov testovaných dát. V prípade potvrdenia normality budú dáta testované parametrickým Studentovým testom. Ak bude normalita vyvrátená, využije sa neparametrický Wilcoxonov test.

Dátum	Dionaea		Tcpdump	
	1	3	4	5
1.6.2015	237	291	289	242
2.6.2015	154	65	57	144
3.6.2015	122	44	51	122
4.6.2015	72	68	66	75
5.6.2015	165	64	58	160
6.6.2015	56	59	66	56
7.6.2015	97	121	123	108
8.6.2015	261	4918	187	270
9.6.2015	272	210	218	264
10.6.2015	167	159	162	163

Dátum	Dionaea	Tcpdump
1.6.2015	528	531
2.6.2015	219	201
3.6.2015	166	173
4.6.2015	140	141
5.6.2015	229	218
6.6.2015	115	122
7.6.2015	218	231
8.6.2015	5179	457
9.6.2015	482	482
10.6.2015	326	325
11.6.2015	663	132

Obr. 4.11 Ukážka analyzovaných dát.

5 Výsledky analýzy dát a teoretický návrh bezpečnostných protiopatrení

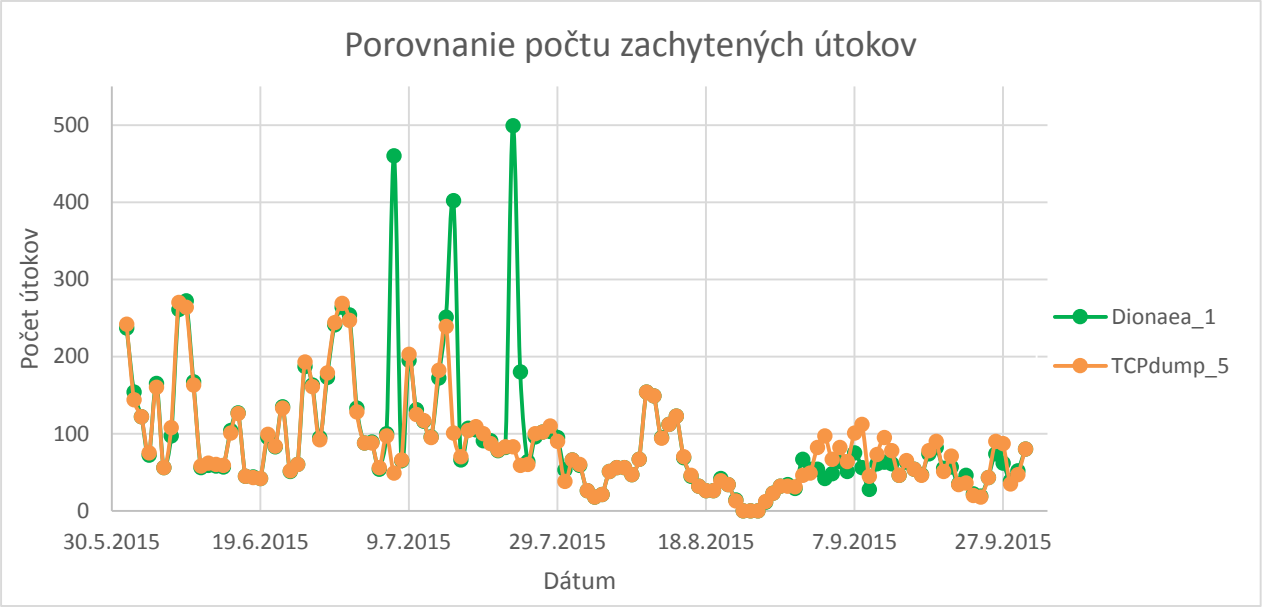
Po tom, ako boli všetky techniky využívané pre spracovávanie dát najskôr overené na testovacej sade dát, môžu sa použiť na plnú sadu dát. Jedná sa o útoky zachytávané po dobu štyroch mesiacov (jún, júl, august, september 2015). Počas tejto doby bolo sondami Dionaea_1, Dionaea_3, Tcpdump_4 a Tcpdump_5 zachytených 44986 útokov.

5.1 Výsledky porovnávania počtu zachytených útokov

Po potvrdení predpokladu na testovacej sade dát o tom, že sonda Dionaea_1 zachytáva rovnaké množstvo útokov ako sonda Tcpdump_5, a sonda Dionaea_3 zachytáva rovnaké množstvo útokov ako sonda Tcpdump_4, bol tento predpoklad overený na plnej sade dát. Pre detailnú a prehľadnú analýzu porovnávania počtu útokov som rovnako, ako v prípade testovacej sady, zvolila porovnávanie útokov zachytených v rámci jedného dňa.

Pred samotnou analýzou plnej sady dát je nutné upraviť ich rozloženie. Z tohoto dôvodu bolo vytvorené makro v programe Microsoft Excel, ktoré automaticky dáta na novom liste s názvom „Počet zachytených správ“ zoradí do prehľadnej tabuľky. Kliknutím na tlačítko „Spustiť porovnávanie dát“ získame dve tabuľky. Prvá obsahuje v jednom stĺpci celkový počet v daný deň zachytených dát sondami typu Dionaea, v druhom stĺpci celkový počet v daný deň zachytených dát sondami typu Tcpdump. V treťom stĺpci sa nachádza rozdiel týchto počtov. Druhá tabuľka zobrazuje pre každý deň počet dát zachytených jednotlivými sondami. Toto makro bolo vytvorené pomocou skript v jazyku Visual Basic. Program prebieha nasledovne: Najskôr sú prejdené všetky záznamy a zistený najstarší a najaktuálnejší dátum útoku. Pre každý dátum sa prejdú všetky záznamy útokov a spočíta sa, koľko útokov zachytených danou sondou sa pre daný dátum v zozname nachádza. Následne sa do daného listu vypíše tabuľka s počtom útokov pre daný dátum a daný typ sondy (Dionaea a Tcpdump) a tiež tabuľka s počtom útokov pre daný dátum pre každú sondu (Dionaea_1, Dionaea_3, Tcpdump_4, Tcpdump_5) zvlášť. V poslednom kroku sa do posledného stĺpca prvej tabuľky vypíše rozdiel počtu zachytených útokov. Z popisu je zrejmé, že nezáleží na množstve spracovávaných dát, jedinou podmienkou pre funkčnosť je zachovanie formátovania tabuľky zdrojových dát. Je preto možné ho využívať aj do budúcnosti. Toto makro sa nachádza v prílohe na CD.

Výsledky porovnávania dát je možné vidieť v Prílohe A v Tabuľke I: Počet zachytených útokov jednotlivými sondami. Ako je zrejmé z grafu 9, sondy Dionaea_1 a Tcpump_5 vyššie uvedený predpoklad spĺňajú. Odchýlka nastáva len v dňoch 7.7., 15.7. a 23.7., kedy došlo k poruche sondy Dionaea_1. Na grafe 10 je vidieť medzi sondami Dionaea_3 a Tcpdump_4 väčší počet odchýlok. Najväčšia odchúlka nastala dňa 8.6., kedy sonda Dionaea_3 z dôvodu poruchy zachytila 4918 útokov (pre zachovanie prehľadnosťi grafu je tento údaj mimo rozsah zvislej osy). Z grafu tak nie je zrejmé, či je vyššie úvedený predpoklad splnený. Pre zistenie bude nutná exploračná analýza a štatistická indukcia.



Obr. 5.1 Porovnanie počtu zachytených útokov – Dionaea_1, Tcpdump_5.

Obr. 5.2 Porovnanie počtu zachytených útokov – Dionaea_3, Tcpdump_4 (detail).

5.2 Výsledky porovnávania útokov na základe krajiny pôvodu – počet útokov

Po potvrdení predpokladu na testovacej sade dát o tom, že sondy typu Dionaea i Tcpdump budú vyhodnocovať krajiny pôvodu zhodne, bol tento predpoklad overený na plnej sade dát. Pred samotnou analýzou plnej sady dát je nutné upraviť ich rozloženie. Z tohoto dôvodu bolo vytvorené makro v programe Microsoft Excel, ktoré automaticky dáta na novom liste s názvom „Krajiny - počet správ“ zoradí do prehľadnej tabuľky. Kliknutím na tlačítko „Spustiť porovnávanie dát“ získame dve tabuľky. Prvá tabuľka obsahuje počet útokov zachytených sondami typu Dionaea rozdelených do stĺpcov podľa toho, z akej krajiny pochádzajú. Druhá tabuľka obsahuje rovnako rozdelené dáta zachytené sondami typu Tcpdump, viz. tabuľka 7. Toto makro bolo vytvorené pomocou skript v jazyku Visual Basic. Program prebieha nasledovne: Najskôr sú prejdené všetky záznamy, čím sa získa zoznam krajín. Pre každú krajinu zvlášť sa prejdú všetky záznamy o útokoch a spočíta sa počet útokov pre sondy typu Dionaea a sondy typu Tcpdump. V poslednom kroku sa do tabuľky zadaného listu vypíše spočítaný počet útokov pre jednotlivé krajiny a jednotlivé typy sond. Z popisu je zrejmé, že nezáleží na množstve spracovávaných dát, jedinou podmienkou pre funkčnosť je zachovanie formátovania tabuľky zdrojových dát. Je preto možné ho využívať aj do budúcnosti. Toto makro sa nachádza v prílohe na CD/DVD.

Na grafe 11 je vidieť, že odchýlky medzi uvedenými krajinami sú len minimálne, najväčšia sa objavuje v prípade USA (US), kedy Dionaea z tejto krajiny zachytila 5938 útokov a Tcpdump 4093 útokov. Táto odchýlka mohla nastať z dôvodu poruchy sondy. Vysvetlivky k skratkám krajín sa nachádzajú v kapitole 4.2.2.

Dionaea													
GB	**DE**	**US**	**FR**	**HK**	**LT**	**NL**	**SA**	**RU**	**AU**	**PS**	**CA**	**--**	**CH**
1325	5938	8533	4437	14	19	664	11	47	12	286	3021	2	123
CN	**MX**	**BE**	**KR**	**SG**	**PH**	**TW**	**IE**	**PL**	**BR**	**VE**	**IN**	**EC**	**NG**
22	3	5	4	19	2	2	1	12	3	1	3	7	4
EG	**NZ**	**VN**	**IR**	**UA**	**CZ**	**RO**	**IS**	**SE**	**QA**	**BO**	**KG**	**PA**	**LU**
49	1	1	2	3	0	21	0	10	1	1	1	1	3

Tcpdump													
GB	**DE**	**US**	**FR**	**HK**	**LT**	**NL**	**SA**	**RU**	**AU**	**PS**	**CA**	**--**	**CH**
1345	4093	7800	3005	17	17	111	13	69	12	335	3162	2	163
CN	**MX**	**BE**	**KR**	**SG**	**PH**	**TW**	**IE**	**PL**	**BR**	**VE**	**IN**	**EC**	**NG**
28	3	2	5	24	2	4	2	10	4	1	4	9	4
EG	**NZ**	**VN**	**IR**	**UA**	**CZ**	**RO**	**IS**	**SE**	**QA**	**BO**	**KG**	**PA**	**LU**
53	1	1	3	4	2	21	1	32	1	1	1	1	3

Tab. 7 Počet útokov na základe krajín.

Obr. 5.3 Porovnanie počtu útokov na základe krajín.

5.3 Výsledky porovnávania útokov na základe krajiny pôvodu – druh útokov

Po potvrdení predpokladu na testovacej sade dát o tom, že sondy typu Dionaea i Tcpdump budú zachytávať zhodné informácie, z ktorých následne neurónová sieť vyhodnotí zhodný typ útokov, bol tento predpoklad overený na plnej sade dát, viz. tabuľka 8. V tejto analýze som sa opäť zamerala na top 5 krajín, z ktorých prichádzalo najviac útokov.

Pred samotnou analýzou plnej sady dát je nutné upraviť ich rozloženie. Z tohoto dôvodu bolo vytvorené makro v programe Microsoft Excel, ktoré automaticky dáta na novom liste s názvom „Krajiny – druh útokov“ zoradí do prehľadnej tabuľky. Kliknutím na tlačítko „Spustiť porovnávanie dát“ získame niekoľko tabuliek. Ich počet závisí od počtu krajín, z ktorých prichádzali útoky. Každá tabuľka predstavuje vždy jednu krajinu a obsahuje počet jednotlivých druhov útokov vyhodnotených z informácií zachytených sondami typu Dionaea (prvá časť tabuľky) a typu Tcpdump (druhá časť tabuľky), viz. tabuľka 8. Toto makro bolo vytvorené pomocou skript v jazyku Visual Basic. Program prebieha nasledovne: Najskôr sú prejdené všetky záznamy, čím sa získa zoznam krajín. Potom sú všetky záznamy prejdené znova, čím sa získa zoznam typov útokov. Následne sa pre každú krajinu zo zoznamu zvlášť prejde získaný zoznam typov útokov, čím sa získa zoznam všetkých kombinácií krajina – typ útoku. Pre každú kombináciu sa prejdú všetky záznamy o útokoch a spočíta sa počet útokov zvlášť pre sondy typu Dionaea a zvlášť pre sondy typu Tcpdump. Takto získané informácie sú v poslednom kroku vypísané do tabuľky zadaného listu. Z popisu je zrejmé, že nezáleží na množstve

spracovávaných dát, jedinou podmienkou pre funkčnosť je zachovanie formátovania tabuľky zdrojových dát. Je preto možné ho využívať aj do budúcnosti. Toto makro sa nachádza v prílohe na CD/DVD.

Krajiny, z ktorých prichádzalo najviac útokov, sa od testovacej sady dát líšia. V prípade plnej sady dát sú týmito krajinami v poradí USA, Nemecko, Francúzsko, Kanada a Veľká Británia. Na grafoch 12 až 16 je vidieť, že odchýlky medzi zachytenými útokmi sú len minimálne

US								
Dionaea	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	4842	2357	6	9	1308	10	1	0
Tcpdump	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	5605	1962	2	14	68	14	134	1

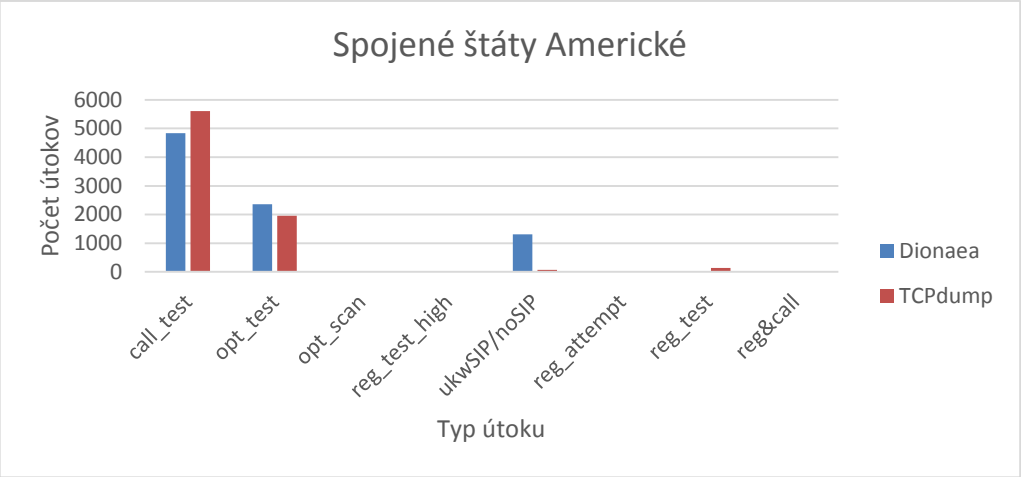
DE								
Dionaea	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	3471	1735	6	20	685	11	5	5
Tcpdump	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	2027	1940	0	24	66	10	20	6

FR								
Dionaea	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	3739	622	2	10	50	14	0	0
Tcpdump	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	2178	736	3	10	15	13	45	5

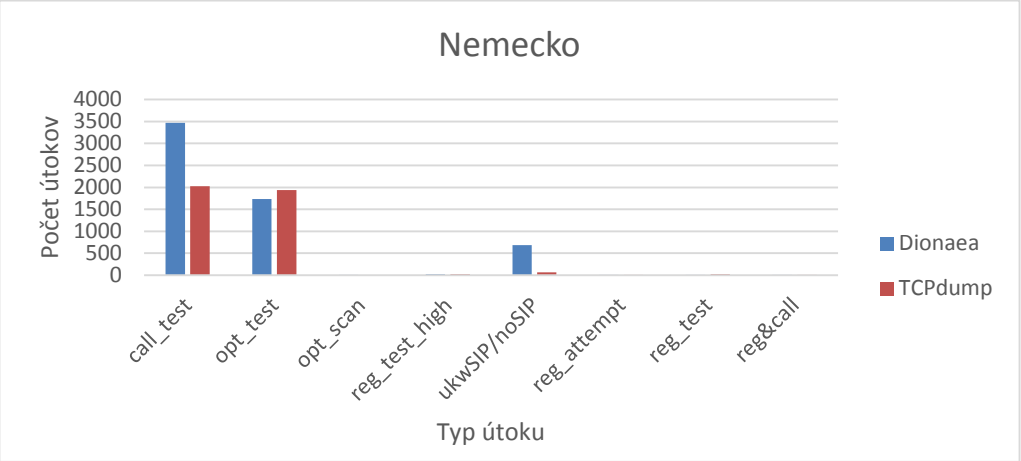
CA								
Dionaea	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	2955	17	0	0	48	1	0	0
Tcpdump	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	3130	23	0	0	6	1	2	0

GB								
Dionaea	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	985	76	1	2	226	3	12	20
Tcpdump	call_test	opt_test	opt_scan	reg_test_high	ukwSIP/noSIP	reg_attempt	reg_test	reg&call
	1163	92	1	3	35	10	6	35

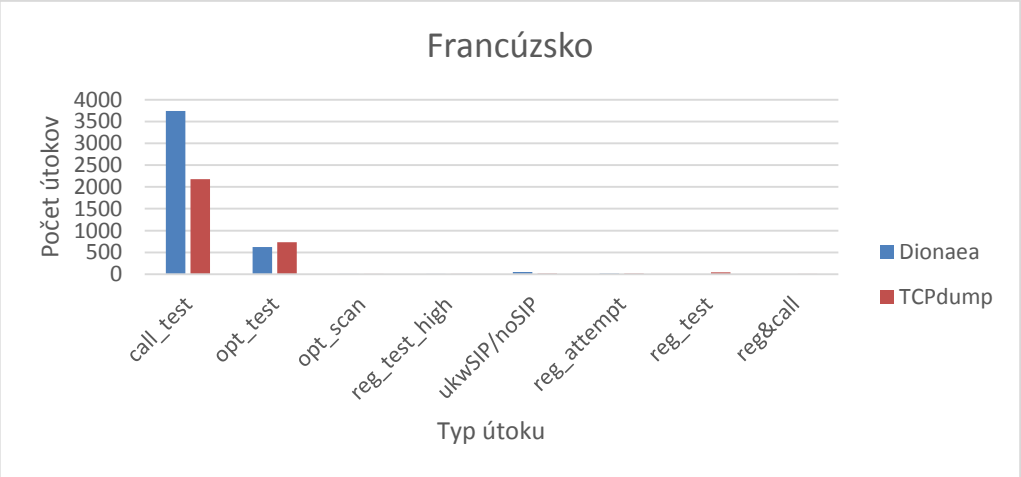
Tab. 8 Porovnanie typu útokov na základe krajín.



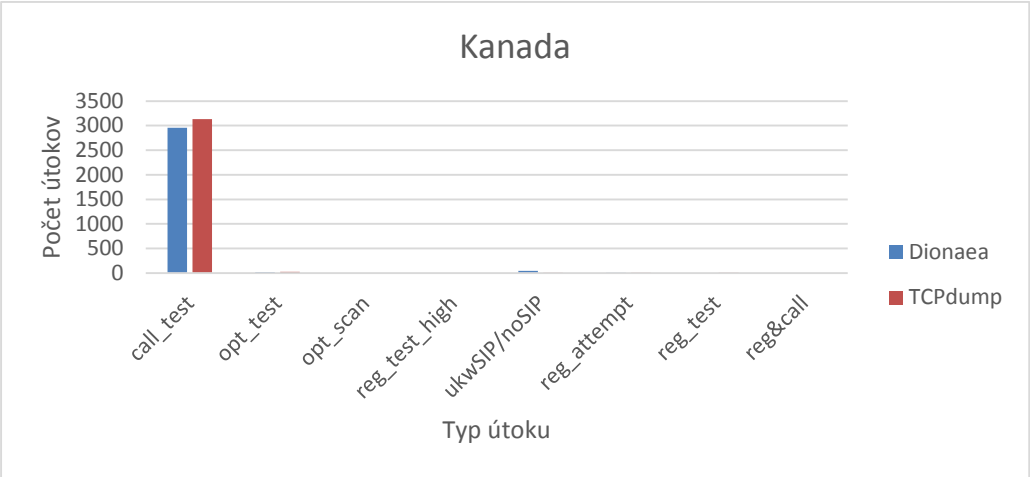
Obr. 5.4 USA, typ útokov.



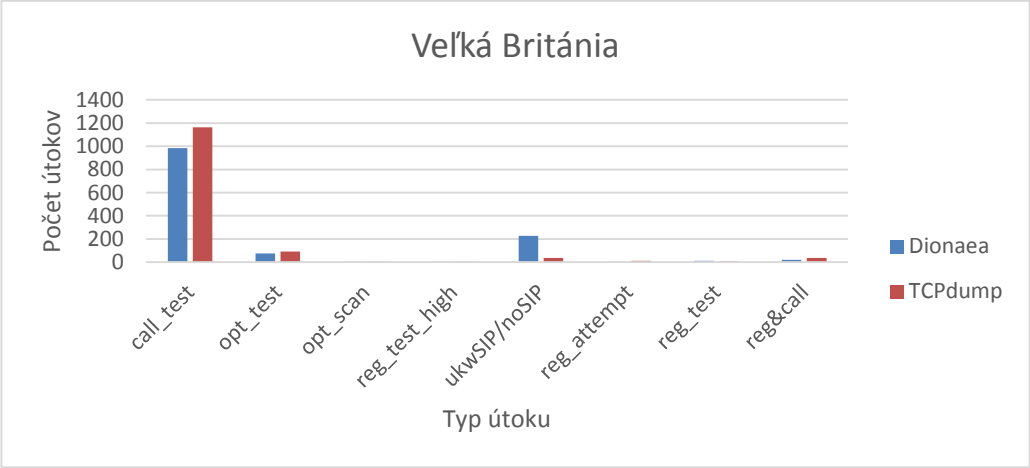
Obr. 5.5 Nemecko, typ útokov.



Obr. 5.6 Francúzsko, typ útokov.



Obr. 5.7 Kanada, typ útokov.



Obr. 5.8 Veľká Británia, typ útokov.

5.4 **Najdlhšie opakovane používané zdrojové IP adresy**

Po tom, ako bolo na testovacej sade dát, že útočníci svoje zdrojové IP adresy využívajú aj opakovane, bola táto informácia overená na plnej sade dát. Teoreticky by sa v nej malo nachádzať približne 22000 rôznych IP adries. Potvrdilo sa, že rovnako ako v prípade testovacej sady dát je väčšina IP adries využívaná na 1-3 útoky len v jeden deň, prípadne na 1 útok trvajúci hodiny až niekoľko dní. Isté množstvo útočníkov ale svoje zdrojové IP adresy využíva opakovane na rovnaký typ útoku. V tabuľke 9 sa nachádza top 10 najvyužívanejších IP adries. V tabuľke 10 je uvedených top 5 skupín IP adries pochádzajúcich z rovnakej siete, ktoré boli na útočenie využívane v rovnaký čas na rovnaký typ útoku. V tomto prípade sa rovnako ako v prípade testovacej sady dát pravdepodobne jednalo o DDoS útok, tj. DoS útok z väčšieho množstva počítačov.

IP adresa	Dátum	Typ útoku	Krajina	
104.193.8.235	7.6., 13.6., 18.6., 20.6., 28.6.	opt_test	US	Pennsylvania
192.99.94.187	8.6., 11.7., 13.7.,	call_test	DE	Germany
5.189.149.123	20.6., 21.6., 27.6., 28.6., 30.6.,	opt_test	US	Missouri
5.189.149.163	2.7., 3.7., 4.7., 7.7., 9.7.	call_test	PS	Palestine
178.162.214.34	2.7., 6.7., 7.7., 8.7., 9.7., 10.7., 12.7., 14.7., 15.7.	opt_test, opt_scan	DE	Germany
195.154.182.229	2.7., 9.7., 13.7., 14.7.	call_test	FR	France
195.154.154.110	8.6., 11.6., 23.7.,	call_test	DE	Germany
209.126.99.80	1.6., 19.8.	call_test	US	New York
212.129.1.25	2.6., 18.7.,	call_test	US	Missouri
37.8.36.196	12.8., 13.8., 16.8.,	call_test	FR	France

Tab. 9 Opakované používanie IP adries.

IP adresa	Dátum	Typ útoku	Krajina	
107.150.32.206 - 107.150.57.91	1.6. - 30.9.	call_test	US	Missouri
109.200.30.32 - 109.200.30.233	17.7. - 16.9	call_test	GB	United Kingdom
199.217.115.21 - 199.217.117.85	1.7. - 17.7.	opt_test	US	Missouri
192.99.66.51 - 192.99.69.165	3.7. - 14.7.	call_test	CA	Quebec
209.58.130.131 - 209.58.130.183	1.6.	call_test	US	New York

Tab. 10 IP adresy rovnakej siete.

5.5 Najvyužívanejší druh útoku

Pre zisťovanie najvyužívanejšieho druhu útoku bola využitá plná sada dát, a to 4986 útokov. V tabuľke 11 je vidieť, až 31508 z nich typu call_test. 9972 útokov je typu opt_test a 2774 útokov bolo vyhodnotených ako uknwSIP/noSIP. Ostatné typy útokov je možné považovať za zanedbateľné. Toto zistenie je prehľadne zobrazené na grafe 17.

Z tejto analýzy vyplýva, že najčastejšie sa útočníci pokúšajú o nadviazanie spojenia pomocou INVITE SIP správ cez vybranú ústredňu. Druhým najčastejším útokom je skenovanie serveru pomocou nižšieho počtu SIP správ OPTIONS, pomocou ktorých sa zisťujú vlastnosti daného SIP zariadenia. Tretí najčastejší útok, ktorý sondy zachytili, neobsahoval SIP správy, respektíve využíval SIP správy iné, než RFC 3261.

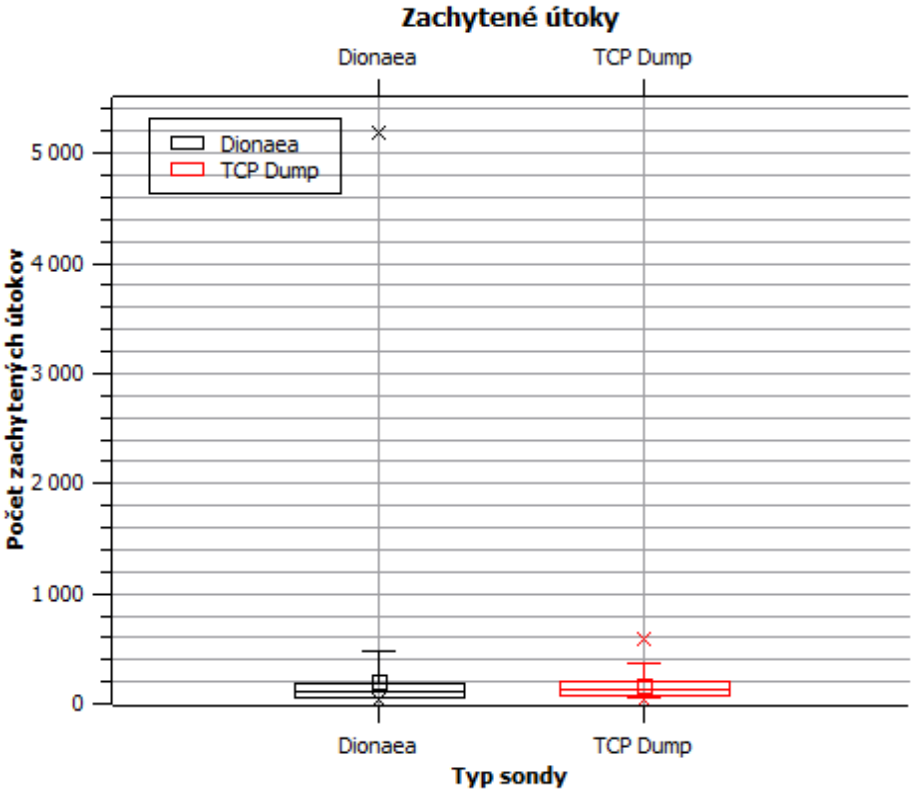
Typ útoku	Počet	Percent [%]
call_test	31508	70,04
opt_scan	24	0,05
opt_test	9972	22,17
reg&call	72	0,16
reg_attempt	234	0,52
reg_test	274	0,61
reg_test_high	128	0,28
uknwSIP/noSIP	2774	6,17
Celkom útokov	*44986*	*100*

Tab. 11 Využívanosť útokov.

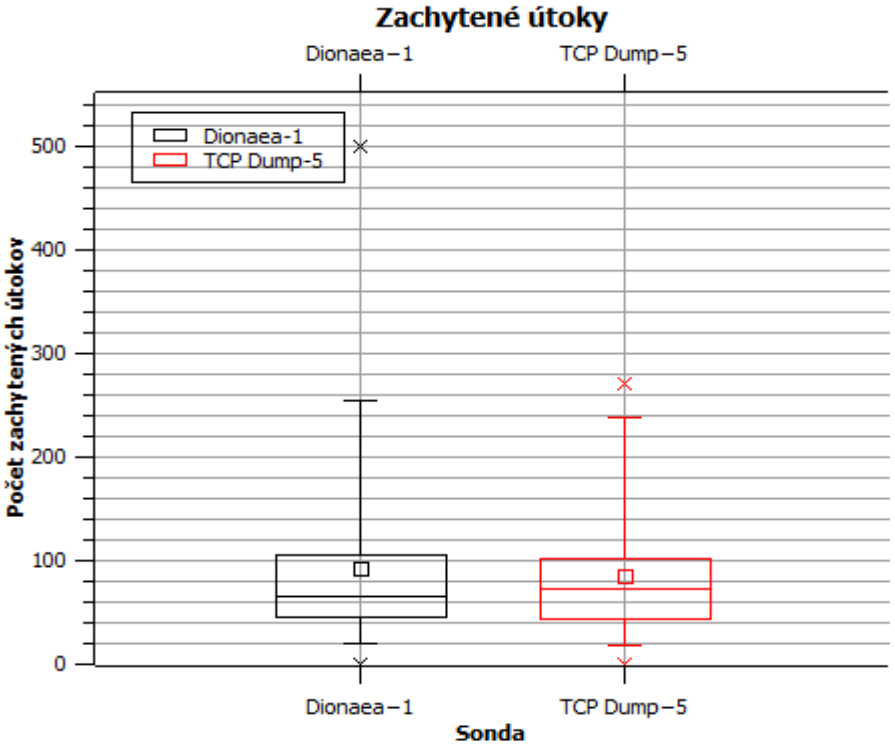
Obr. 5.9 Využívanosť útokov.

5.6 Výsledky štatistickej analýzy dát

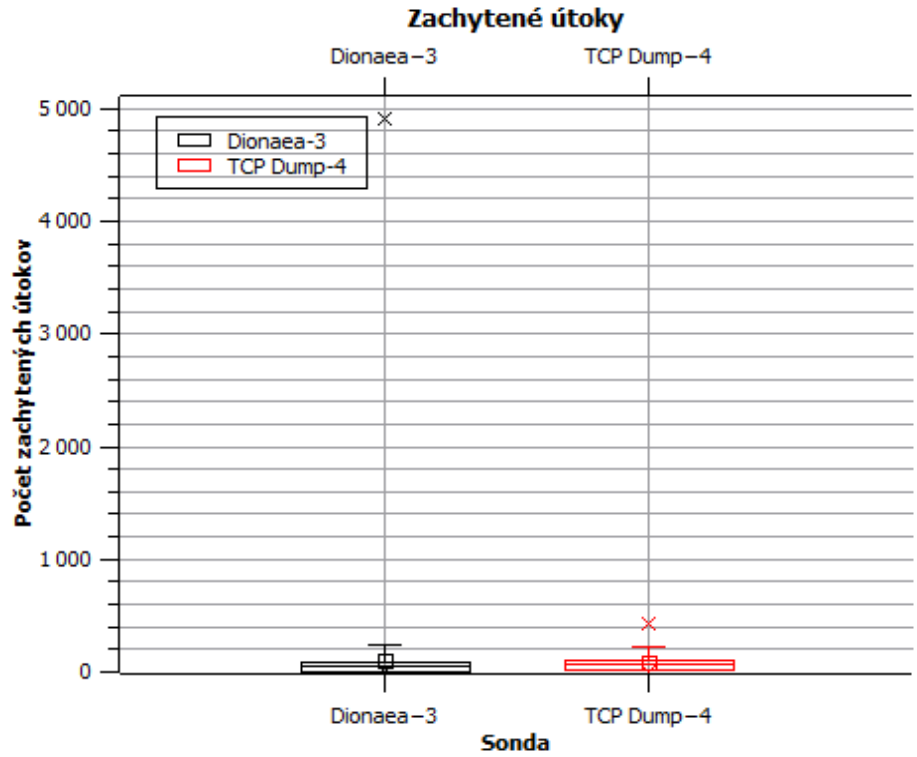
V prvom kroku analýzy boli pre porovnávané dvojice sond vytvorené krabicové grafy. Z grafu 19, na ktorom je zobrazený krabicový graf porovnávajúci sondy Dionaea_1 a Tcpdump_5 je zrejmé, že pre rozdiely medzi sondami by nemali byť štatisticky významné. Na grafoch 18 ktorom je zobrazený krabicový graf porovnávajúci sondy typu Dionaea so sondami typu Tcpdump. Kvôli veľkým odľahlým pozorovaniam však graf nie je dostatočne prehľadný na to, aby bol vidieť rozdiel medzi sondami. Rovnako je to aj v prípade grafu 20, na ktorom je zobrazený krabicový graf porovnávajúci sondy Dionaea_3 so sondou Tcpdump_4. V tabuľke 12 sa nachádza charakteristika sond po tom, ako boli z dát odstránené odľahlé pozorovania.



Obr. 5.10 Krabicový graf pre sondy typu Dionaea a Tcpdump.



Obr. 5.11 Krabicový graf pre sondy Dionaea_1 a Tcpdump_5.



Obr. 5.12 Krabicový graf pre sondy Dionaea_3 a Tcpdump_4.

	Dionaea	Tcpdump	Dionaea_1	Tcpdump_5	Dionaea_3	Tcpdump_4
Počet útokov	121	122	119	122	120	122
Maximum zachytených	778	589	272	270	291	435
Minimum zachytených	34	34	0	0	0	0
Medián	119	136,5	64	72	49,5	63

Tab. 12 Charakteristika sond.

Normalita dát (Gaussovo rozloženie) bola overená pomocou Shapiro-Wilkovho testu. Na hladine významnosti 0,05 bola normalita vo všetkých prípadoch zamietnutá, viz. tabuľka 13. Pre overenie rozdielnosti súborov testovaných dát tak bude nutné použiť neparametrický Wilcoxonov test.

	P-hodnota
Dionaea	$4{,}005*10^{-13}$
Tcpdump	$1{,}088*10^{-9}$
Dionaea_1	$3{,}29*10^{-9}$
Dionaea_3	$1{,}61*10^{-10}$
Tcpdump_4	$3{,}57*10^{-12}$
Tcpdump_5	$1{,}26*10^{-8}$

Tab. 13 Shapiro-Wilkov test.

Po použití neparametrického dvoj hodnotového Wilcoxonovho testu bolo zistené, že rozdielnosť dát zachytávaných sondami Dionaea_1 a Tcpdump_5 nie je štatisticky významná. Štatisticky významné rozdiely sú však medzi sondami Dionaea_3 a Tcpdump_4. Tak isto tomu je aj vo všeobecnom porovnávaní medzi sondami typu Dionaea a sondami typu Tcpdump, viz tabuľka 14.

	P-hodnota
Tcpdump vs Dionaea	< 0,0001
Tcpdump_5 vs Dionaea_1	0,062
Tcpdump_4 vs Dionaea_3	< 0,0001

Tab. 14 Wilcoxonov test.

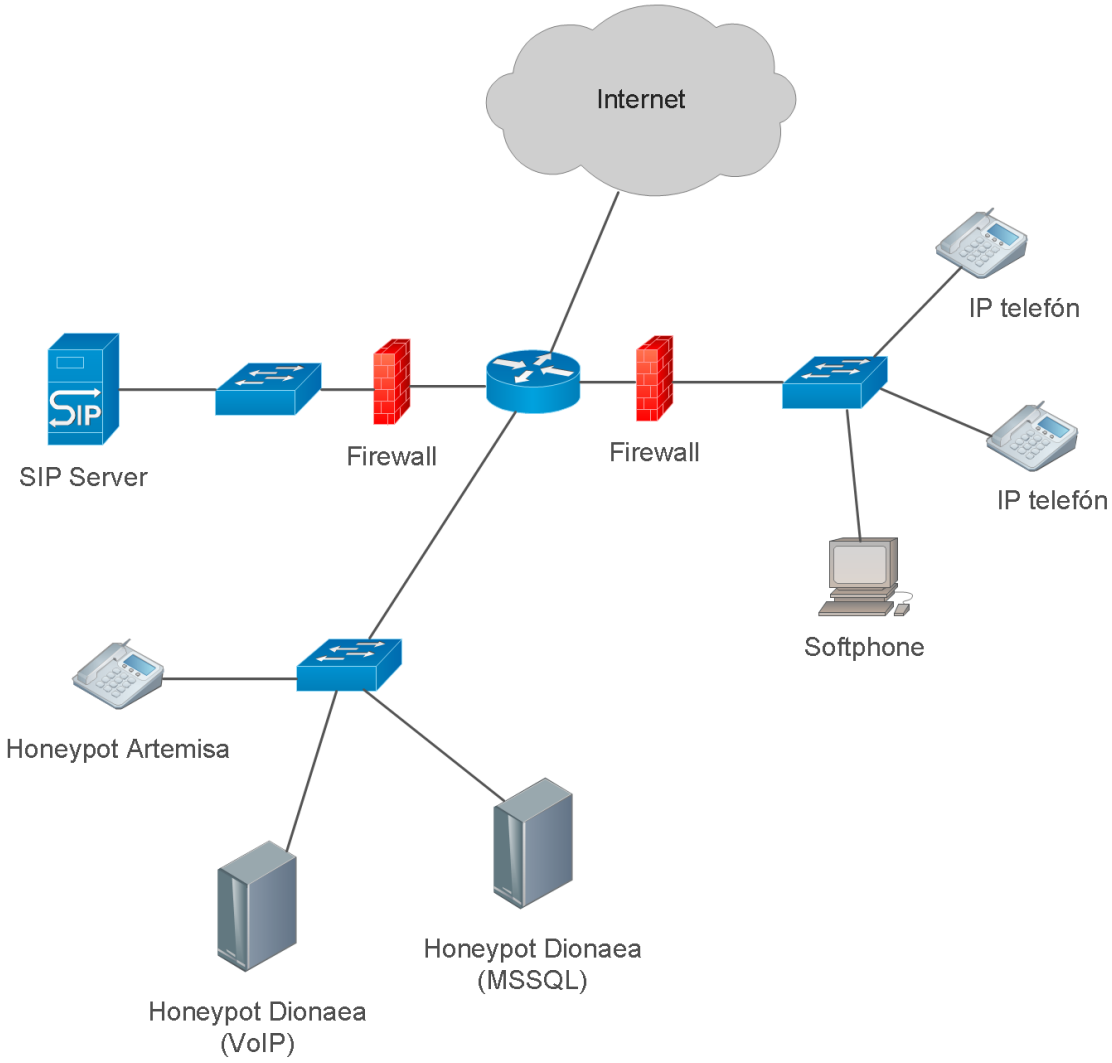
Na základe výsledkov tejto štatistickej analýzy dát môžeme tvrdiť, že sondy Dionaea_1 a Tcpdump_5 zachytávajú v rámci dní rovnaké množstvo dát, a teda pracujú efektívne. Inak je tomu v prípade sond Dionaea_3 a Tcpdump_4, medzi ktorými boli zistené štatisticky významné rozdiely. Toto zistenie pravdepodobne vyplýva z opakovaných porúch sondy Dionaea_3 v období, z ktorého analyzované dáta pochádzajú. Spôsobov, ako analyzovať tento súbor dát, je veľké množstvo, záleží od toho, aké informácie potrebujeme zistiť. V budúcnosti by bolo možné napríklad porovnávať vlastnosti sond rovnakého typu pomocou Friedmanovho testu.

5.7 Teoretický návrh vhodných bezpečnostných protiopatrení

Na základe prevedených analýz bolo úlohou poslednej kapitoly navrhnúť vhodné bezpečnostné protiopatrenia pre sieť s VoIP infraštruktúrou. Z výsledkov tejto práce vyplýva, že útočníci sa zameriavajú najmä na narušanie bezpečnosti pomocou skenovania siete. Jedná sa o identifikáciu aktívnych účtov na SIP pobočkovej ústredni pomocou SIP žiadostí INVITE a OPTIONS. Je možné predpokladať, že ďalším cieľom útočníkov bude v takýchto prípadoch prelomenie hesiel zistených účtov napríklad útokmi hrubou silou.

Vhodným bezpečnostným protiopatrením pomocou honeypotov vo VoIP infraštruktúre by mohla byť kombinácia honeypotov Artemisa a Dionaea. Artemisa simuluje koncový bod siete, narozdiel od Dionaey, ktorá je schopná simulovať rôzne služby ako VoIP, HTTP, FTP či MSSQL. Tieto ďalšie služby môžu byť pre útočníka zaujímavé pri zisťovaní názvov účtov a hesiel. Kombináciou všetkých by sa dalo zaručiť, že honeypoty nalákajú útočníkov s rôznymi možnými cieľmi. Zaistilo by sa tak nie len odvedenie pozornosti od dôležitých sieťových prvkov, ale aj získavanie širokej škály informácií o útokoch. Na základe toho by bolo možné vytvárať efektívne aktualizované zabezpečenie a útoky tak obmedziť či úplne eliminovať. Na obrázku 5.1 je návrh takejto siete, pričom podsieť s honeypotmi úmyselne nie je od ostatných oddelená firewallom. Stáva sa tak oproti ostatným podsieťam ľahšie prístupnejšou a tým aj lákavejšou pre útočníkov.

V praxi by bolo najefektívnejšie okrem vyššie spomenutých bezpečnostných nástrojov využívať aj také, ktoré nie sú zamerané výhradne na VoIP infraštruktúru. Jedným z takýchto nástrojov je honeypot Kippo, ktorý je vyvinutý na simuláciu SSH (Secured Shell) serveru. Bolo by tiež napríklad možné doplniť sieť o IDS/IPS (Instruction Detection System/Instruction Prevention System) zariadenie určené pre monitoring siete s využitím identifikácie škodlivej činnosti a následným blokovaním. Okrem týchto bezpečnostných nástrojov by bolo vhodné oddelit VoIP infraštruktúru od ostatnej siete pomocou VLAN (Virtual Local Area Network). Vznikla by tak logicky oddelená sieť, čím by sa jej bezpečnosť zvýšila.



Obr. 5.13 Návrh bezpečnostných protiopatrení.

Záver

Hlavným cieľom tejto diplomovej práce bola analýza dát z VoIP honeypotov nasadených v reálnej sieti s vysokou intenzitou prevádzky, definícia najčastejšie používaných typov útokov a teoretický návrh vhodných bezpečnostných protiopatrení. Úvod práce bol venovaný základným pojmom IP telefónie a protokolom technológiou Voice over IP, ktorými sú hlavne signalizačný protokol SIP, transportný RTP protokol a ich bezpečnostné mechanizmy. Druhá kapitola sa zaoberala problematikou bezpečnostných rizík vo VoIP SIP telefónii, ktorými sú monitoring a manipulácia so signalizáciou, či útoky ako Man in the Middle a DoS. V ďalšej časti bol definovaný pojem honeypot, jeho využitie a delenie do rôznych kategórií. Boli popísané nástroje pre implementáciu VoIP honeypotov Artemisa a Dionaea a tiež paketový analyzér Tcpdump. Vo štvrtej kapitole bol čitateľ zoznámený s podkladmi meraní a tiež so základným popisom neurónovej siete. Následne bola táto kapitola venovaná spôsobom, ktorými boli dáta analyzované. Jednalo sa o porovnávanie počtu zachytených útokov rôznymi sondami, ich pôvodu, zisťovanie najvyužívanejšieho typu útoku na VoIP technológiu a popis exploračnej analýzy a štatistickej indukcie. V záverečnej časti boli uvedené jednotlivé výsledky analýzy dát a tiež teoretický návrh vhodných bezpečnostných protiopatrení.

Pre zjednodušenie analýzy dát boli pre túto prácu vytvorené makra v programe Excel, ktoré potrebné dáta formátujú do prehľadných tabuliek. Tieto makra je možné využívať pre analýzu aj v budúcnosti, jedinou podmienkou pre funkčnosť je zachovanie formátovania tabuľky zdrojových dát. Tieto makra by v prípade potreby bolo možné v budúcnosti rozšíriť o ďalšie metódy analýzy dát. V rámci tejto diplomovej práce bolo zistené, že najčastejším typom útoku na VoIP infraštruktúru je call_test, čo znamená, že sa útočníci pokúšajú o nadviazanie spojenia pomocou INVITE SIP správ cez vybranú ústredňu, a to až priemerne v 80% zo všetkých útokov. Štatistickou analýzou dát bolo zistené, že rozdielnosť počtu útokov zachytávaných sondami Dionaea_1 a Tcpdump_5 nie je štatisticky významná. Štatisticky významné rozdiely sú však medzi sondami Dionaea_3 a Tcpdump_4. Toto zistenie pravdepodobne vyplýva z opakovaných porúch sondy Dionaea_3 v období, z ktorého analyzované dáta pochádzajú. Vzhľadom k týmto záverom verím, že hlavné ciele diplomovej práce boli splnené.

Použitá literatúra

[1] Miroslav Vozňák, "Spojovací systémy", Vysokoškolské skriptá, VŠB-TU Ostrava, 2012, ISBN 978-80-248-1961-7

[2] Miroslav Vozňák, Filip Řezáč, "Voice over IP", VŠB-TU Ostrava, 2010

[3] Filip Řezáč, "Zabezpečená komunikace na SIP protokolu", Diplomová práca, VŠB-TU Ostrava, 2009

[4] Jakub Šafařík, Filip Řezáč, Miroslav Vozňák "Monitoring of Malicious Traffic in IP Telephony Infrastructure", CESNET z.s.p.o., Praha, 2012

[5] Niels Provos, Thorsten Holz, "Virtual Honeypots: From Botnet Tracking to Intrusion Detection", ISBN: 978-0321336323

[6] Jakub Safarik, Miroslav Voznak, Filip Rezac, Pavol Partila, Karel Tomala, "Automatic Analysis of Attack Data from Distributed Honeypot Network", Ostrava

[7] Filip Řezáč, Miroslav Vozňák, Jan Rozhon, "Bezpečnost v komunikacích", Ostrava, 2013

[8] Lance Spitzner, "Honeypots: Tracking Hackers" ISBN: 978-0321108951

[9] Miroslav Vozňák, "Technologie a protokoly multimediálních komunikací pro integrovanou výuku VUT a VŠB-TUO", Ostrava, 2014

[10] P. Zimmermann, "ZRTP: Media Path Key Agreement for Unicast Secure RTP", apríl 2011

[11] Divya and Sanjeev Kumar, "Analysis of Denial of Service Attackss in IEEE 802.11s Wireless Mesh Networks", India 2009

[12] Artemisa v1.0 documentation, http://artemisa.sourceforge.net/, marec 2016

[13] Emil Tan, "Dionaea – A Malware Capturing Honeypot", http://www.edgis-security.org/honeypot/dionaea/, marec 2016

[14] Tcpdump & Libpcap, http://www.tcpdump.org/, marec 2016

[15] Jakub Safarik, Miroslav Voznak, Miralem Mehic, Pavol Partila, Martin Mikulec, "Neural network classifier of attacks in IP telephony", Ostrava

[16] Ing. Jakub Šafařík, "Distribuovaný systém klasifikace útoků pro VoIP infrastrukturu využívající protokol SIP", Teze dizertační práce, Ostrava 2014

[17] Excel Macros&Programming, http://www.excel-vba.com/, február 2016

[18] M. Collier, D. Endler - Hacking Exposed Unified Communications & VoIP Security Secrets & Solutions, Second Edition, 2013

[19] The Honeynet Project, http://www.honeynet.org/, február 2016

[20] VOIP Security Aliance, http://www.voipsa.org/, február 2016

[21] SIP: Session Initiation Protocol, "https://www.ietf.org/rfc/rfc3261.txt", február 2016

[22] RTP, "http://www.voip-info.org/wiki/view/RTP", február 2016

[23] RTP: A Transport Protocol for Real-Time Applications, "https://tools.ietf.org/html/rfc3550", február 2016

[24] VOIP Security, http://www.voip-info.org/wiki/view/VOIP+Security, marec 2016

[25] Matthew Ruck, "Top Ten Security Issues Voice over IP (VoIP)", 2010

[26] Honeypot Concepts, http://www.honeyd.org/concepts.php/, marec 2016

[27] E. Peter, T. Schiller, "A Practical Guide to Honeypots", http://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html, marec 2016

[28] F.El-moussa, P.Mudhar, A. Jones, "Overview of SIP Attacks and Countermeasures", Edith Cowan University, Perth 2009

[29] MS Excel: VBA Functions – Listed by cathegory, "http://www.techonthenet.com/excel/formulas/index_vba.php", marec 2016

[30] Introduction to the Visual Basic Programming Language, "https://msdn.microsoft.com/library/xk24xdbe(v=vs.90).aspx", marec 2016

[31] QtiPlot – Data Analysis and Scientific Visualisation, "http://www.qtiplot.com/", apríl 2016

[32] GraphPad Software, "http://www.graphpad.com/", apríl 2016

Zoznam príloh

Príloha na CD.

Adresárová štruktúra priloženého CD:

Data:	Plná sada analyzovaných dát
Makra:	Makra vytvorené pre zjednodušenie analýzy získaných dát
Text:	Text diplomovej práce

Príloha A: *Tabuľka I: Počet zachytených útokov jednotlivými sondami.*

Dátum	Dionaea		Tcpdump	
	1	3	4	5
1.6.2015	237	291	289	242
2.6.2015	154	65	57	144
3.6.2015	122	44	51	122
4.6.2015	72	68	66	75
5.6.2015	165	64	58	160
6.6.2015	56	59	66	56
7.6.2015	97	121	123	108
8.6.2015	261	4918	187	270
9.6.2015	272	210	218	264
10.6.2015	167	159	162	163
11.6.2015	56	607	74	58
12.6.2015	59	64	63	62
13.6.2015	58	20	28	60
14.6.2015	57	0	133	59
15.6.2015	104	0	162	101
16.6.2015	127	0	59	126
17.6.2015	45	0	23	45
18.6.2015	44	0	21	43
19.6.2015	42	0	15	42
20.6.2015	95	0	24	99
21.6.2015	83	0	17	84
22.6.2015	135	0	24	133
23.6.2015	51	0	22	52
24.6.2015	60	0	26	60
25.6.2015	187	0	26	193
26.6.2015	163	0	27	161
27.6.2015	95	0	20	92
28.6.2015	173	0	15	179
29.6.2015	241	0	17	244
30.6.2015	264	12	26	269
1.7.2015	254	127	130	247
2.7.2015	133	157	159	128
3.7.2015	88	165	164	88
4.7.2015	89	102	97	88
5.7.2015	54	99	101	56
6.7.2015	100	144	145	97
7.7.2015	460	84	87	49
8.7.2015	65	80	74	66
9.7.2015	195	72	74	203
10.7.2015	131	237	244	125
11.7.2015	116	251	246	117
12.7.2015	96	139	139	95
13.7.2015	172	88	87	182
14.7.2015	251	89	81	239
15.7.2015	402	260	149	101
16.7.2015	66	122	121	70
17.7.2015	107	109	110	104
18.7.2015	105	63	63	109
19.7.2015	91	29	26	100
20.7.2015	91	62	62	87

21.7.2015	78	83	86	79
22.7.2015	82	65	63	83
23.7.2015	499	279	61	83
24.7.2015	180	33	34	59
25.7.2015	64	56	57	60
26.7.2015	96	63	68	100
27.7.2015	102	165	160	102
28.7.2015	103	63	190	110
29.7.2015	95	22	79	90
30.7.2015	53	47	47	38
31.7.2015	66	67	67	66
1.8.2015	59	60	60	60
2.8.2015	26	62	62	26
3.8.2015	18	38	38	18
4.8.2015	21	30	31	21
5.8.2015	51	23	23	51
6.8.2015	56	33	33	56
7.8.2015	56	18	18	56
8.8.2015	47	21	21	47
9.8.2015	67	24	24	67
10.8.2015	154	218	435	154
11.8.2015	149	194	386	149
12.8.2015	95	72	144	94
13.8.2015	112	67	134	112
14.8.2015	123	43	86	123
15.8.2015	69	33	64	70
16.8.2015	45	39	78	46
17.8.2015	32	50	102	32
18.8.2015	26	48	96	26
19.8.2015	26	48	91	26
20.8.2015	42	42	46	39
21.8.2015	34	34	34	34
22.8.2015	14	35	35	13
23.8.2015	0	36	37	0
24.8.2015	0	34	34	0
25.8.2015	0	56	122	0
26.8.2015	11	107	280	12
27.8.2015	23	89	89	23
28.8.2015	32	184	184	32
29.8.2015	34	105	105	32
30.8.2015	29	25	26	31
31.8.2015	67	0	0	46
1.9.2015	54	3	3	49
2.9.2015	54	21	79	82
3.9.2015	42	34	92	97
4.9.2015	48	58	67	67
5.9.2015	64	22	74	82
6.9.2015	51	0	43	64
7.9.2015	75	0	19	101
8.9.2015	56	10	24	112
9.9.2015	28	33	36	45
10.9.2015	61	60	58	73
11.9.2015	63	53	54	95
12.9.2015	61	23	23	78

13.9.2015	46	16	30	46
14.9.2015	63	36	63	65
15.9.2015	54	92	65	54
16.9.2015	47	57	52	46
17.9.2015	74	82	79	78
18.9.2015	82	88	122	90
19.9.2015	55	40	47	51
20.9.2015	57	61	110	71
21.9.2015	35	49	72	34
22.9.2015	46	33	34	36
23.9.2015	22	28	28	20
24.9.2015	19	21	27	18
25.9.2015	43	63	63	43
26.9.2015	74	79	77	90
27.9.2015	62	62	65	87
28.9.2015	39	42	39	35
29.9.2015	52	43	43	47
30.9.2015	80	62	76	80

Príloha B: *Tabuľka II: Porovnanie zachytených útokov Dionaea vs Tcpdump.*

Dátum	Dionaea	Tcpdump
1.6.2015	528	531
2.6.2015	219	201
3.6.2015	166	173
4.6.2015	140	141
5.6.2015	229	218
6.6.2015	115	122
7.6.2015	218	231
8.6.2015	5179	457
9.6.2015	482	482
10.6.2015	326	325
11.6.2015	663	132
12.6.2015	123	125
13.6.2015	78	88
14.6.2015	57	192
15.6.2015	104	263
16.6.2015	127	185
17.6.2015	45	68
18.6.2015	44	64
19.6.2015	42	57
20.6.2015	95	123
21.6.2015	83	101
22.6.2015	135	157
23.6.2015	51	74
24.6.2015	60	86
25.6.2015	187	219
26.6.2015	163	188
27.6.2015	95	112
28.6.2015	173	194
29.6.2015	241	261

30.6.2015	276	295
1.7.2015	381	377
2.7.2015	290	287
3.7.2015	253	252
4.7.2015	191	185
5.7.2015	153	157
6.7.2015	244	242
7.7.2015	544	136
8.7.2015	145	140
9.7.2015	267	277
10.7.2015	368	369
11.7.2015	367	363
12.7.2015	235	234
13.7.2015	260	269
14.7.2015	340	320
15.7.2015	662	250
16.7.2015	188	191
17.7.2015	216	214
18.7.2015	168	172
19.7.2015	120	126
20.7.2015	153	149
21.7.2015	161	165
22.7.2015	147	146
23.7.2015	778	144
24.7.2015	213	93
25.7.2015	120	117
26.7.2015	159	168
27.7.2015	267	262
28.7.2015	166	300
29.7.2015	117	169
30.7.2015	100	85
31.7.2015	133	133
1.8.2015	119	120
2.8.2015	88	88
3.8.2015	56	56
4.8.2015	51	52
5.8.2015	74	74
6.8.2015	89	89
7.8.2015	74	74
8.8.2015	68	68
9.8.2015	91	91
10.8.2015	372	589
11.8.2015	343	535
12.8.2015	167	238
13.8.2015	179	246
14.8.2015	166	209
15.8.2015	102	134
16.8.2015	84	124
17.8.2015	82	134
18.8.2015	74	122
19.8.2015	74	117
20.8.2015	84	85
21.8.2015	68	68
22.8.2015	49	48

23.8.2015	36	37
24.8.2015	34	34
25.8.2015	56	122
26.8.2015	118	292
27.8.2015	112	112
28.8.2015	216	216
29.8.2015	139	137
30.8.2015	54	57
31.8.2015	67	46
1.9.2015	57	52
2.9.2015	75	161
3.9.2015	76	189
4.9.2015	106	134
5.9.2015	86	156
6.9.2015	51	107
7.9.2015	75	120
8.9.2015	66	136
9.9.2015	61	81
10.9.2015	121	131
11.9.2015	116	149
12.9.2015	84	101
13.9.2015	62	76
14.9.2015	99	128
15.9.2015	146	119
16.9.2015	104	98
17.9.2015	156	157
18.9.2015	170	212
19.9.2015	95	98
20.9.2015	118	181
21.9.2015	84	106
22.9.2015	79	70
23.9.2015	50	48
24.9.2015	40	45
25.9.2015	106	106
26.9.2015	153	167
27.9.2015	124	152
28.9.2015	81	74
29.9.2015	95	90
30.9.2015	142	156